Safety Analysis Guide

1. Introduction

The safety policy of the Lawrence Livermore National Laboratory (LLNL) is to take every reasonable precaution in the workplace to protect the environment and the health and safety of employees and the public, and to prevent property damage. Thus, the design, construction, management, operation, and maintenance of LLNL facilities, activities, and projects must be undertaken to limit those risks to acceptable levels.

This policy is based on the U.S. Department of Energy (DOE) Organization Act, which requires documented evidence of environment, safety, and health (ES&H) considerations in facility / project design and operation. DOE Order 5480.1B, *Environment, Safety, and Health Protection Program for DOE Operations*, interprets the Organization Act by defining DOE programs to achieve the objectives set forth. One program is the Safety Analysis and Review System (SARS) for which requirements are given in DOE Order 5481.1B. This Order specifies requirements, responsibilities, and guidance for the preparation and review of safety analyses. The requirements are sufficiently general to allow field organizations to implement their own programs to satisfy the basic requirements. The comparable field office directives are DOE-SAN Management Directives (MDs) 5480.1A and 5481.1A.

1.1 Purpose

This Guide describes the LLNL SARS and presents guidelines for the preparation, review, and approval of safety analyses. The guidelines given here will help ensure that LLNL safety analyses fulfill the following:

- Safety Analysis Reports (SARs) must adequately demonstrate that activities are conducted in accordance with ES&H objectives.
- They should conservatively bound activities while realistically modeling operations and postulated events.
- SARs are consistently and efficiently prepared.

This document is a guide instead of a manual and, thus, it is not a "cookbook." Details of how to perform each specific analysis are not presented. Rather, the available resources are discussed, and a system and logical framework provided for analysis and documentation.

1.2 Contents

Section 2 presents background information on the LLNL SARS, including requirements, basic criteria, a brief overview of how the LLNL SARS functions and its organization and responsibilities. Section 3 includes a recommended approach to performing and documenting safety analyses, making various estimates, and other concerns (e.g., design criteria and cost and scheduling activities). Supporting information such as summaries of analysis tools and format and content is presented in the appendices.

2. Safety Analysis and Review System

The LLNL SARS stems from DOE Order 5481.1B whose stated purpose is: "To establish uniform requirements for the preparation and review of safety analyses of DOE operations, including identification of hazards, their elimination or control, assessment of the risk, and documented management authorization of the operation." DOE-SAN MD 5481.1 implements the order, establishes format and content for SARs, and provides guidance relative to using various analytical techniques.

The main orders and management directives that control and guide safety analyses are:

DOE Order	SAN MD
5481.1B	5481.1A (draft)
5480.1B	5480.1A
5480.5	5480.5
5480.4	
5480.16	
6430.1A	

Appendix A of this Supplement gives a short summary of the basic contents of these documents, as well as highlights of SAR requirements, DOE Order 5481.1B, and DOE Order 6430.1A.

Note: *The wording used in most of this section is taken directly from the various orders, manuals, guides, and directives that control safety analysis activities. They are abbreviated but are presented as complete and unadulterated as possible to avoid misrepresentation.*

2.1 Basic Requirements

2.1.1 General

The basic SAR requirements are stated in DOE Order 5481.1B. These requirements are implemented at the (SAN) field office level by MDs. The general requirements of the DOE Order for the line organization include:

1. Prepare appropriate safety analyses for each DOE operation and subsequent significant modifications, including decommissioning.
2. Independently review each safety analysis (field organization or contractor internal reviews may be used).
3. Provide appropriate authorization for the construction, operation, and subsequent significant modifications, including decommissioning, of each DOE operation.
4. Provide DOE with the safety analysis when available and, concurrent with an authorization, the completed review(s) that establish the authorization basis.
5. Maintain the official DOE file of all pertinent documentation regarding the authorization.

In short, the process breaks down into safety analysis, review, authorization, and documentation. The Order also describes basic requirements for these activities, which are summarized in more detail in the following sections. Only those requirements that concern SAR content and preparation are discussed.

2.1.2 Safety Analysis

Safety analyses must:

1. Be initiated during the earliest phases of the operation to facilitate early hazard identification and elimination or control.
2. Be provided by the organization with immediate operating responsibility.
3. Identify and demonstrate conformance with applicable guides, codes, and standards.
4. Wherever possible, cover classes of operations within a facility so that individual operations are bounded by the general analysis.
5. Describe design and operational features that demonstrate conformance with environmental assessments or impact statements.

Also, it is part of Contract 48 between the University of California and the DOE that a SAR is prepared before the initial startup of a nuclear facility and before any startup following a change that represents a significant deviation from the procedures, equipment, or analyses in the SAR.

2.1.3 Review

The review shall:

1. Evaluate the adequacy of preventive or mitigative design features and administrative controls that have been provided to limit risk.
2. Be conducted by individuals, the majority of whom are not directly involved in the management of the DOE operation evaluated.
3. Be sufficiently documented to allow independent evaluation of its adequacy.

2.1.4 Authorization

The authorization must:

1. Signify that the risk has been determined to be acceptable.
2. Limit a DOE operation to those characteristics described and analyzed in the safety analysis.

2.1.5 Documentation

All pertinent details of the analysis, review, and authorization relative to any DOE operation shall be traceable from the initial identification of a hazard to its elimination or the application of controls necessary to appropriately reduce the risk. (Evidence of conformance with the design shall be incorporated in appropriate sections of the safety analysis report, or as an appendix for existing reports at the next update.)

2.2 Applicability

Figure 2-1 shows a general idea of which activities are required to have a safety analysis. Exclusions include routinely encountered hazards (e.g., gasoline filling stations), nuclear safety of weapons designs, work activities that are exclusively construction-related, and the OSHA program. No clear rules are available to determine whether or not a hazard is routinely accepted (i.e., does not present an unusual hazard). Some characteristics that may make hazards unusual are materials or energy sources that are:

- Associated with "dread fear" in the general population.
- Not incorporated into common settings or daily life.
- Used in magnitudes, or result in potential releases, that are much larger than previously used in industrial applications (or may present catastrophic consequences).
- Used in an untested application.

Characteristics that may be used to determine hazards are routinely accepted, *not* unusual, include:

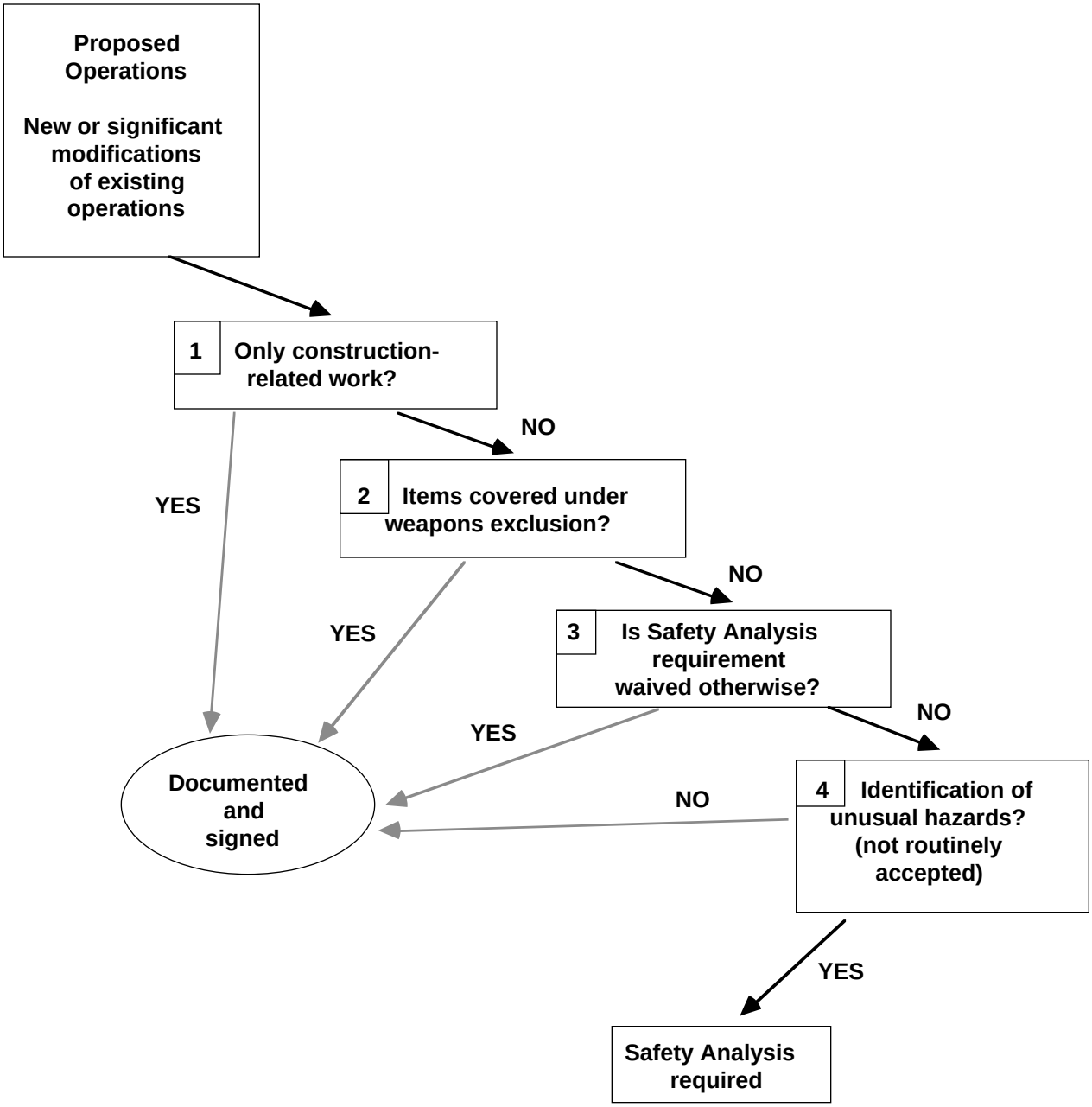


Figure 2-1. Safety analysis requirements for proposed operations.

- The hazard is routinely encountered first-hand by the general public in the home, home workshop, or in public areas.
- Public consensus standards exist to control the hazard.
- No evidence exists that there are public or employee concerns about the hazard beyond the normal prudence.

An example of an operation that may be considered "routinely accepted" is a gasoline filling station on a DOE site for fueling government vehicles. However, a filling station for hydrogen-powered vehicles would, most likely, represent an unusual hazard.

The safety assessment for an operation or project that involves hazards of a type and magnitude routinely encountered and accepted by the public may require no more than a formal statement such as: "This project / operation involves only hazards of a type and magnitude routinely encountered and accepted by the public, and no additional analysis is required." The final authority for making this determination lies with the appropriate DOE-SAN line management.

If a safety analysis is deemed necessary (from Fig. 2-1), the analysis activities and the review and authorization levels depend on the hazard classification. Facilities or operations are categorized in DOE 5481.1B according to hazard class as follows:

Low Potential for minor on-site and negligible off-site impacts to people or to the environment.

Moderate Considerable potential for on-site impact to people or the environment, but at most only minor off-site impact.

High Potential for on-site or off-site impact to large numbers of people or for major impact to the environment.

Hazard classes specific to nuclear facilities are defined in SAN MD 5480.5 and in Section 2.5.1 of this Supplement. Hazard classification is discussed in Section 3.1.

The documentation (Safety Analysis Report [SAR] or Safety Analysis Document [SAD]) requirements for the various hazard classes are:

	Non-Nuclear Project			Nuclear Project	
Hazard class	**Low**	**Mod.**	**High**	**Mod.**	**High**
Document required	SAD	SAD	SAR	SAR	SAR

A short description of the contents of these documents follows in the next section. The definition of a "nuclear facility" is discussed in Section 2.5.1, and means that a Low hazard category would be a misnomer.

2.3 Basic Documents

Preliminary Hazard Analysis (PHA). A PHA characterizes the hazard in terms of cause, location, frequency, mitigation, prevention, and impact early in project life. The PHA provides the basis for a tentative hazard class and can be used in the SAD or SAR, below.

Safety Assessment Document (SAD). A SAD documents the formal analysis of potential hazards for all low hazard and moderate hazard non-nuclear facilities or operations. The conclusions and results should support the hazard class, identify additional analyses if necessary, and risk type and magnitude. A recommended outline and content is given in Appendix B.

Safety Analysis Report (SAR). A SAR is a formal document that describes a facility or operation and the safety analysis. This document provides reasonable assurance that the activity can be performed with acceptable risk to public health and safety and with adequate protection of operating personnel, material, and the environment. A SAR is required for all high hazard and all moderate hazard nuclear facilities or operations. The SAR for complex operations or projects is usually developed in two stages with the preliminary SAR (PSAR, below) submitted just before construction and the final SAR (FSAR, below) submitted just before operation. A recommended outline and content is given in Appendix B.

Preliminary Safety Analysis Report (PSAR). A PSAR is prepared during project design. The analysis is based primarily on functional requirements, design criteria, and conceptual and detailed design. A PSAR objective is to determine whether the design has sufficiently considered safety features so the project may be operated safely. The PSAR should contain adequate information to identify all elements of the project and the safety systems required in the design. The PSAR should also describe the basis on which these systems were selected. The PSAR contains adequate background data to assure sufficient funding for the required safety systems. The safety analysis will be completed to the level of detail allowed by existing design information.

Final Safety Analysis Report (FSAR). An FSAR completes documentation of the analysis begun as a PSAR. The FSAR addresses how the findings of the PSAR were implemented in the final design. For ongoing facilities / projects that require a SAR, an FSAR will be the only document prepared and approved. The FSAR should include detailed information on facility operation, as well as the organizational responsibility for each operation, all personnel training programs, and all inspection, testing, safety system maintenance, and quality assurance requirements.

Facility Safety Procedures (FSPs). FSPs are the basic safety ground rules to be followed by all personnel present within a building or area. They must be reviewed at least every three years.

Operational Safety Procedures (OSPs). OSPs, used primarily by experimenters, are generally more limited in scope and more specific in content than FSPs. They must be reviewed annually.

2.4 Organization

This section identifies key organizations for input to, and preparation, review, and approval of, safety analysis documents within LLNL.

Line Organizations. Projects, programs, and / or facility organizations are responsible for safety analysis requirements for their operations and to manage and prepare appropriate safety analysis documents. Safety analysis activities are discussed in Section 2.5.

Hazards Control Department. The Health and Safety (H&S) Division of the Hazards Control

Department provides guidance and services to managers and employees on health and safety matters. The relationship between the H&S Division and line organizations for SAR activities is shown on Fig. 2-2.

The safety team is the line organization's primary interface with the Hazards Control Department. As necessary, the Safety Team Leader can obtain help from the discipline groups and the staff SAR advisor. The advisor can provide guidance on how to:

- Determine if a SAR is required.
- Assess hazard classification.
- Estimate manpower and budget requirements.
- Assemble a preparation team.
- Arrange for review, submit for approval, resolve comments.

Other advisor services include briefings on and interpretation of SAR requirements, and establishing and maintaining a library of reports, orders, guides, examples of model SARs, and contractor information. This guide was prepared and is maintained by the staff SAR advisor.

Other. At times, other support may be needed from within LLNL and should be arranged on a case-by-case basis. This support may include:

- Environmental impact assessment (Environmental Guidance and Monitoring Division of the Environmental Protection Department).
- Reliability and maintainability analysis and risk assessment (Risk Assessment and Reliability Engineering Group, Systems Research Group).
- Radiological release dose estimation (Atmospheric Release Advisory Capability).
- Structural analysis (Plant and Technical Services, Plant Engineering).
- Document production (Technical Information Department).
- Quality assurance.

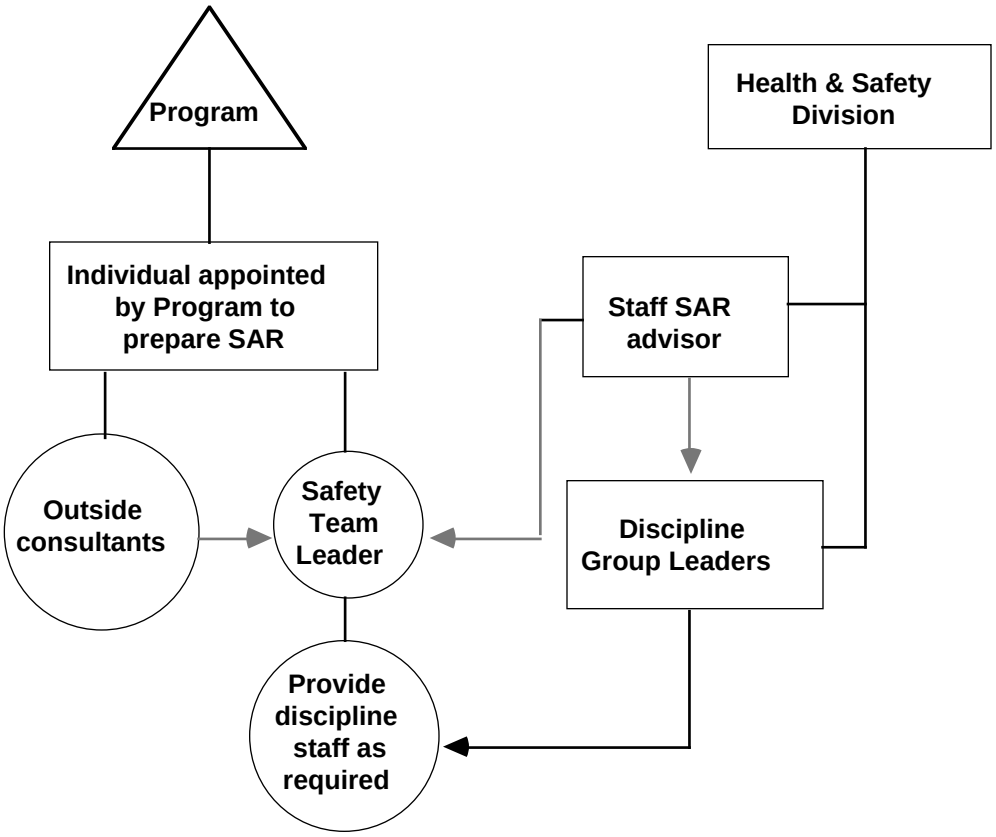


Figure 2-2. Safety analysis organizational relationships.

2.5 Safety Analysis and Review System Tasks

The system at LLNL for preparing, reviewing, approving, and controlling safety analyses is the LLNL SARS. The depth and extent of analysis, documentation, and review activities depend on project complexity and the hazard class.

Safety analysis activities are shown in Table 2-1. Not all activities are needed for all safety analyses. However, most activities are needed in some form for most analyses. The relationship of safety analysis to project phases for most new projects is shown on Fig. 2-3. Table 2-1 and Figure 2-3 point out that safety analyses can be complicated, require prior planning, and should be started early in the project.

2.5.1 Estimate Effort

The first step is for the project or program to assign a manager for the safety analysis activities. This provides a line of authority and responsibility as well as a single focal point for inquiries.

The first analysis activity should be a PHA culminating in a preliminary hazard classification, since the hazard class can have a significant impact on project design and safety analysis documentation, review, and approval requirements. Thus, estimating the safety analysis effort requires at least a preliminary hazard classification. The PHA provides support for this classification. The hazard classification will be verified or modified in the actual safety analysis.

Note: Modifying a hazard classification later in the project can be difficult and costly, so the PHA is an important step that should be carefully performed. DOE-SAN agreement on the hazard class should be obtained as early as possible.

The general hazard class definitions from DOE 5481.1B are as follows:

Low Potential minor on-site and negligible off-site impacts to people or the environment.

Moderate Considerable potential on-site impact to people or the environment, but at most only minor off-site impact.

High Potential on-site or off-site impacts to large numbers of people or for major impact to the environment.

DOE Order 5480.5 defines:

Nuclear Facilities are those facilities involving radioactive materials in such form and quantity that a

Table 2-1. Typical Safety Analysis Activities

Phase 1 — Estimate Effort

1. Line organization assigns a SA manager.
2. Perform preliminary hazards analysis.
3. Determine preliminary hazard classification and inform DOE (even if exempt).
4. Determine document and resource requirements and schedule.
5. Obtain support from the Hazards Control Department or outside consultant.

Phase 2 — Perform and Document Analysis

6. Assign a writing and analysis team.
7. Perform hazard identification and characterization, safety analysis, criteria and risk assessment, OSR determination, etc.
8. Prepare the draft.
9. Perform document quality check.

Phase 3 — Review and Approval

10. Submit for Hazards Control Department review and approval.
11. Revise as needed.
12. Submit for LLNL line/institutional review and approval.
13. Revise as needed.
14. Submit for DOE review and approval as needed.
15. Revise as needed.

Phase 4 — Maintenance

16. Publish the document.
17. Periodically review and update if safety envelope has changed.

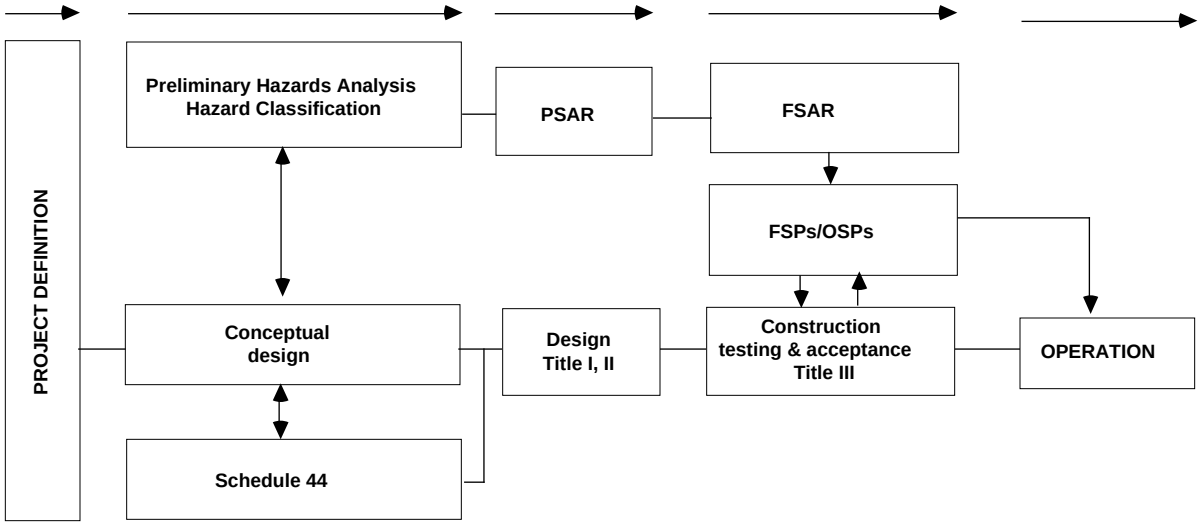


Figure 2-3. Relationship of safety documentation to project phases for new projects.

significant nuclear hazard potentially exists to employees or public. Included are facilities that: (1) produce, process, or store radioactive liquid or solid waste, fissionable materials, or tritium; (2) conduct separation operations; (3) conduct irradiated materials inspection, fuel fabrication, decontamination, or recovery operations; or (4) conduct fuel enrichment.

High Hazard Non-Reactor Nuclear Facilities are those for which the calculated consequence of *any credible accident (no mitigation factors assumed)* could result in any of the following:

1. A committed effective dose equivalent (CEDE) to any individual located off-site in excess of 20 rem from all possible pathways within the first ten days following the accident. The following meteorological assumptions are to be used in the dose calculations:
   - Worst-case atmospheric stability classification.
   - Average ground wind speed of one meter per second.
2. The off-site contamination levels, eight or more hours after initial deposition, exceed the levels below over an area of 100 square meters or greater.
   - 3.5 μCi / m^2 for transuranic isotopes.
   - 35 μCi / m^2 for all other alpha-emitting isotopes.
   - 40 mrad / h at 1 cm for beta / gamma radiation.
3. A dose in excess of 20 rem to 100 persons or more located on site.
4. The on-site contamination levels exceed the levels above over an area of one square kilometer or greater.

Moderate Hazard Non-Reactor Nuclear Facilities for which the calculated radiological consequence of *any credible accident* could result in any of the following:

1. A dose in excess of 20 rem to five persons or more located on site.
2. The on-site contamination levels exceed the levels above over an area of 100 m^2 or greater.
3. A CEDE in excess of 5 rem to any individual located off site.
4. The off-site contamination levels exceed 1 / 10 the levels above over an area of 100 m^2 or greater.

Currently, no specific DOE guidance is available for determining the hazard classification of non-nuclear facilities by assessing non-radiological consequences. Due to the complexity of the subject matter, clear numerical limits that represent the general definitions of DOE 5481.1B are probably not achievable. The Industrial Hygiene Group of the H&S Division should be consulted for guidance in classifying non-nuclear facilities and projects.

2.5.2 Perform and Document Analysis

A team should now be assembled to work on the safety analysis. Depending on the identified hazards and workload priorities, Hazards Control Department

Table 2-2. Safety analysis distribution and review.

EXEMPT/EXCLUDED
Plant Engineering Manager for project
Safety Team Leader
HC discipline(s) involved
SAR advisor file
Environmental Protection Department
Program / Client Safety Analysis Manager

LOW
All of the above, plus
H&S Division
HC Department
AD for Plant & Technical Services or designee
Cognizant AD or designee
DOE-SAN (information only—2 copies)

MODERATE
All of the above, plus
QA Office
DOE-SAN (review and approval—2 copies)

HIGH
All of the above, plus DOE-SAN forwards to DOE-HQ for review and approval

personnel can provide the needed support. The line organization should prepare the design criteria and facility or process description portions.

The facility, systems, materials, and operations including decommissioning should be researched to define and bound the subject of the analysis. First, all hazards are characterized using energy source and hazard identification tables. These tables include likelihood, consequence, safety systems, mitigation and prevention, causes, and location.

Next, hazards are grouped by category (i.e., fire, explosion, natural phenomena, etc.), severity, and likelihood (normal operation, off-normal incident, accident, design basis accident). Other tasks may include computer estimation of event probabilities and consequences. The hazard characteristics are then compared with criteria to determine if they are controlled properly and the risk is acceptable. Barriers, controls, and all assumptions should be clearly identified. Some of these will result in OSRs. DOE guidance on content and format should be followed.

In addition, conformance with applicable guides, codes, and standards must be demonstrated. Deviations must be evaluated and documented. More details on the process, methods commonly used, and format and content are presented in Section 3.

2.5.3 Review and Approval

The line organization is also responsible for managing the safety analysis review, which should be ordered as follows: writing team review, HC safety team and discipline review, HC and line management review, and institutional review (as needed). Institutional review consists of reviews for environmental, legal, and / or consistency issues. A distribution and review chain is given in Table 2-2. The review and approval levels are given in Table 2-2a.

Form LL 4337, Pre-Publication Review (shown in Fig. 2-4), is used to record reviews up to the AD level. For AD and DOE levels, the Safety Analysis and Review System Documentation Form (Fig. 2-5) is used. Also, SAN MD 5480.5 states "for high hazard nuclear facilities and selected moderate hazard facilities, cognizant Program Senior Official approval with the Office of the Assistant Secretary for ES&H concurrence must be obtained prior to authorization." That approval can take six months or more, depending on workload and sensitivity. Thus, a long review and resolution period is expected for safety analyses submitted to DOE-HQ.

The review and approval process provides: (a) an independent check on the analysis against requirements, (b) a documented evaluation of the adequacy of the preventive or mitigative design features and the administrative controls provided to limit the risk, (c) a management acceptance of risk, and (d) approvals for project advancement through phase milestones. The review must be sufficiently documented to allow independent evaluation of its adequacy.

2.5.4 Maintenance

Safety analysis documentation must be updated when the facility is "significantly modified," or for any change involving an unreviewed safety question (USQ). The USQ criteria are:

- The probability of occurrence or the consequences of an accident or malfunction of equipment important to safety evaluated previously will be significantly increased, or
- A possibility for an accident or malfunction of a different type than any evaluated previously will

Table 2-2a. Review and approval levels.

Hazard Class	Review Level	Authorization Level
High	SAN and / or HQ	SAN and / or HQ
Moderate	SAN and / or HQ	SAN and / or HQ
Low	LLNL	LLNL

be created that could result in significant safety consequences.

In addition, FSARs for nuclear facilities should be reviewed by the program or project at a maximum interval of five years (according to draft DOE SAN MD 5481.1A) to determine if the FSAR is adequate and reflects current usage. If at this time the FSAR safety envelope is no longer bounding, the FSAR should be updated and, where practicable, using the format given in Appendix B.

3. Guidance

This section gives guidance on conducting various safety analysis activities. The guidance should help ensure the safety analysis meets applicable criteria, presents realistic and bounding estimates, and is prepared efficiently.

3.1 Hazard Classification

The hazard classification affects: structure, system, and component safety classification;[1] SAR format and content; and the SAR review and approval chain. The hazard classification is based on worst-case consequences from credible accidents.

Hazard classification does not define or consider risk. Usually, when the hazard classification is being determined project design is just starting, and safety features and controls have not been determined. It is important to note the difference between preventive and mitigative features. *Preventive* features control the event frequency, and *mitigative* features control the level of consequences once the event is postulated to occur. Credit may be taken for mitigative features when the risk is being determined, but no credit may be taken for mitigative features when the hazard class is being determined. This section discusses different approaches to determining hazard classification.

3.1.1 Methods

The factors that control hazard class are accident credibility and source term. Hazards are the energy or hazardous material source terms released by credible accidents. Early in the project, the hazard posed by such sources should be clearly stated, independent of mitigation. Regardless of controls, a cylinder of highly toxic gas is a more significant hazard than a cylinder of O_2. Since the hazard is more significant, control requirements should be stricter, and the subsequent safety analysis and risk assessment should be more detailed. Also, the safety documentation should receive additional attention through a higher-level review and approval process.

If credit were allowed for mitigative features, all facilities would be in the low hazard class. The controls for mitigating accidents involving an oxygen release would be designed the same as for a release of highly toxic gas. This level of control is not appropriate for the hazard involved.

Note that the hazard classification is not a statement of the risk of operating that facility. The statement of risk is the conclusion of the safety analysis on the detailed design (which includes mitigative features). Safety features (design or administrative) control the level of risk associated with a hazard. Controls are determined from the risk assessment, design criteria, and standards.

One way to determine hazard level is to assume a worst-case, that the maximum amount of hazardous material is instantaneously released to the environment. If this approach still results in a low hazard class, no more work needs to be done on hazard classification. However, while simple and easy to perform, the source term in this estimate may not be credible.

The source term selected should not violate physical principles. Credit can be taken for the actual amount of material at risk rather than assuming that *all* is available for release. The actual amount at risk may be less than the maximum available if credit can be taken for *passive* barriers that will withstand worst-case (but credible) accident conditions. If the release is inside a building, applicable and conservative release parameters such as release fraction, building holdup, release rate, or dilution could be used to determine the source term. If the accident occurs outside the building, building holdup or dilution would not be relevant.

In any case these physical parameters are different from active safety systems designed for consequence mitigation. Features such as ventilation, filtration, and sprinkler systems; seismic-actuated valves; alarms and recovery team activities are not used to determine hazard class. These features can be used later in the safety analysis to reduce the risk.

The same facility can have multiple hazard classifications. Each area can be designed appropriately to control its hazard level. However, design and safety criteria and accident analyses need to be carefully addressed. A lower safety class component must not cause failure of a higher-rated item.

Consider a building that contains radioactive materials within welded cans in one area. The cans are subjected to nondestructive analysis. That area is separated from the rest of the building by a fire barrier capable of withstanding any *credible* fire. The accident with the worst consequences is a fire that causes the cans to burst and make the radioactive material airborne. The area has an HVAC system complete with HEPA filters that exhaust through a building stack. This HVAC system is independent of the rest of the building and is designed in accordance with DOE

Figure 2-4. Pre-Publication Review Form.

Figure 2-5. Safety Analysis and Review System documentation form.

Order 6430.1A. The area structure and necessary safety-related components are Design Basis Earthquake (DBE) rated.

One way to determine hazard class is to postulate that every can bursts, and the entire amount of radioactive material becomes airborne and is released to the environment. This approach is conservative and results in the largest source term. It may be acceptable if the results are relatively benign. However, future program changes (large increases in the numbers of cans in the area) could result in expensive backfitting and analysis later. Also, this simple approach may set a precedent for other projects where such conservativism may not be appropriate and may result in significant cost increases relative to the hazard level.

Another approach is to assess the credibility of the accident and determine a realistic and conservative source term for the release. For now, assume the Design Basis Fire (DBF) is credible. If no credible mechanism can breach the physical passive barrier during the DBF, then a fire-caused release does not have to be considered and another accident can be assessed. If, however, the cans may burst, a source term should be developed. Rather than assume all the radioactive material is consumed and is released to the environment, credit may be taken for the physical process involved in the DBF. For example, only a portion of the radioactive material located near the breach may become airborne. Further, either physical laws or experimental results can provide limits on the amount of material (release fraction or rate, or maximum airborne concentration) that actually becomes airborne. Some credit may be taken for airborne particulate "plate out" on building surfaces as well. However, estimates of the amount at risk, release fraction or rate, concentration, and plate out *must be conservative and supportable.* No credit can be taken for the HEPA-filtered HVAC system or for an elevated (stack) release. The result will be lower consequences than by assuming the entire inventory is instantaneously released outside the building; the result will still be bounding consequences, though, because a credible, conservative source term is used that does not take credit for mitigative features.

Note, this approach must be *carefully* considered. It is *not* valid if cans are handled outside the building, or opened inside the building, or if barrier integrity is successfully challenged in *any* credible way (e.g., credible aircraft impact, human error, credible earthquake-caused building collapse). Credible events are those events with a probability rate greater than 10^{-6}/yr. The assessment must remain conservative and must satisfy the intent of hazard class terminology. Finally, the hazard class will be verified or modified in the safety analysis. Taking classification shortcuts early may result in expensive retrofits if a higher class is mandated later.

3.1.2 Preliminary Hazards Analysis

The PHA is a precursor to further hazard and safety analysis, and is intended to be used only in the early phases of project development. A PHA focuses on the hazardous materials and major project elements, since details on design or procedures are not yet likely to be available. Normally, the PHA contains the rationale for the hazard classification, generating a list of hazards related to raw materials and products, facility and equipment, system and component interfaces, and operations and operating environment. The PHA is basically a review of where energy or hazardous materials can be released in an uncontrolled manner.

The LLNL *Health and Safety Manual*, Chapter 2, Appendix 2-A contains a list for determining the hazards that may be present. This list is presented in Table 3-1. Other examples are given in Appendix C of this Supplement.

Once the potential hazards have been identified from the PHA and the source term developed, the impacts onsite and offsite are estimated for comparison with the hazard level criteria, as in Section 2.5.1. Guidance on estimating consequences is presented in Section 3.5. Some of the assumptions unique to hazard class determination are: ground release (no credit for HVAC operation), worst-case atmospheric stability, and 1 m/s average ground wind speed. Other assumptions, such as conservative inhalation class, dose conversion factors, can also be made.

3.2 Format and Content

Format guidance is outlined in DOE-SAN MD 5481.1A (draft), which makes distinctions among hazard classes. Low hazard class and non-nuclear moderate hazard projects should prepare a SAD with seven chapters.

1. Introduction.
2. Summary and Conclusions.
3. Description of Site, Facility, and Operations.
4. Safety Analysis.
5. Operational Safety Requirements.
6. Quality Assurance.
7. References.

Not all of these topics may be necessary (i.e., OSRs). In that case only a simple statement is needed. The content for the topics is specified in the MD and contained in Appendix B of this Supplement.

SARs are prepared for all high hazard non-nuclear and high and moderate hazard nuclear projects. "Low" hazard nuclear does not exist. The recommended format is:

1. Introduction and General Description of Installation.
2. Summary Safety Analysis.

3. Site Characteristics and Environmental Protection.
4. Principal Design Criteria.
5. Facility Design.
6. Process Description.
7. Waste Confinement and Management.
*8. Analysis of Normal Operations.
9. Accident Analysis.
10. Conduct of Operations.
11. Operational Safety Requirements.
12. Quality Assurance.
13. References and Acknowledgments.
14. Other Government Agency Jurisdiction.

* This chapter differs from the SAN MD in order to incorporate non-radiological safety programs and normal operational impacts.

The content for this format is also presented in Appendix B of this Supplement. Specific topic guidance is also presented in applicable NRC regulatory guides (e.g., RG 3.26 for fuel reprocessing plants). For the SAR format, every topic should be addressed.

Document length depends on hazard class and project complexity. Regardless of its length, a formal analysis of potential hazards must be performed and documented. The results and conclusions should support the hazard classification, and the magnitude and acceptability of risk. Details may be placed in references or appendices. However, the document should contain enough material so that a reviewer can assess the adequacy of the analysis and the conclusions. References should be retrievable.

Draft guidance is being developed by Los Alamos National Laboratory for DOE-HQ on the format and

Table 3-1. Hazard energy source list.

Electrical Sources
- Capacitors
- Transformers
- Batteries
- Exposed conductors
- Static electricity
- Other high-voltage sources

Motion Sources
- Pulley, belts, gears
- Shears, sharp edges, pinch points
- Vehicles
- Mass in motion

Gravity-Mass Source
- Falling
- Falling objects
- Lifting
- Tripping, slipping
- Earthquakes

Pressure Sources
- Confined gases
- Explosives
- Noise
- Chemical reactions
- Stressed mechanical systems

Cold Sources
- Cryogenic materials
- Ice, snow, wind, rain

Chemical Sources
- Corrosive materials
- Flammable materials
- Reactive materials
- Pathogenic materials (virus, bacteria, etc.)
- Oxygen deficiency
- Carcinogenic material

Heat Sources
- Electrical
- Steam
- Flames
- Solar
- Friction
- Chemical reactions
- Spontaneous combustion

Radiant Sources
- Intense light
- Lasers
- Ultraviolet
- X rays and ionizing radiation
- Infrared sources
- Electron beams
- Magnetic fields
- RF fields
- Nuclear criticality

content of DOE SARs. That draft guidance is available for information from the SAR advisors of the H&S Division. Useful ideas and information from the draft guidance have been incorporated into this Supplement. Specific content guidance is presented in the remainder of this section for the topics of safety systems, safety programs, accident scenarios, and emergency planning.

3.2.1 Safety Systems

Design Criteria. Criteria that apply to the facility and process equipment and engineered systems are to be listed in SARs. The equipment and engineered systems are those that support the overall safety functions of the facility and those that are specific to individual processes, operations, or isolated areas in a facility. Types of systems that are included are:

Facility

- Confinement barriers and systems.
- Effluent treatment systems.
- Ventilation and off-gas systems.
- Specific equipment and instrumentation.
- Radiation shielding.
- Monitoring and alarm systems.
- Fire and explosion protection or mitigation systems.

Process

- Nuclear criticality prevention systems.
- Waste handling / treatment systems.
- Vessels and piping.
- Industrial and chemical safety systems if beyond those normally encountered in industrial settings.

The codes, standards, and guides applicable to those systems should be identified.

Descriptions. The SAR should include detailed descriptions of features, equipment, and systems that are important to safety. These descriptions should include design or performance criteria, interfaces with other equipment or systems, and conditions under which the equipment or systems must function for normal operations, abnormal occurrences, and accident conditions. A list of the Design Basis Accidents and accident scenarios that determine the performance criteria should be provided.

As an example of the design or performance criteria to be included, consider a ventilation and off-gas system:

- Air-flow patterns and velocity with respect to contamination control.
- Minimum negative pressures to maintain proper flow control.
- Interaction of off-gas systems with ventilation systems (bleed-off rate, etc.).
- Minimum filter performance (particulate removal efficiency, maximum pressure drop).
- Minimum performance of any other toxic material removal equipment.
- Minimum performance of dampers and instrumented controls.
- Minimum standards to ensure continuity of operation or safe shutdown under appropriate accident conditions.

If codes and standards are part of the performance or design criteria, indicate whether the codes and standards are being applied as intended and consistent with proven practice. Where codes and standards are being applied in a non-standard manner, explanation and evaluation of studies done to validate these applications should be provided.

The contents should provide a clear understanding of the measures taken to protect workers, the public, and the environment. These protective measures collectively act to detect, prevent, or mitigate unsafe conditions.

3.2.2 Safety Programs

In the SAR, each safety program should be described in sufficient detail to demonstrate that the programs are appropriate and comprehensive in controlling the hazards of the operation to the extent determined necessary by the safety analysis. Some safety programs may control standard industrial hazards. These programs should be described to the extent that their failure or function has an effect on the safety of operations involving unusual hazards. Typical programs that should be addressed are listed below.

Radiation Protection Programs. Describe the radiation protection programs developed for the operation. The topics should include:

- As Low As Reasonably Achievable (ALARA) policy and program.
- External radiation exposure control.
- External dosimetry.
- Internal radiation exposure control.
- Internal dosimetry.
- Radiological protection instrumentation.
- Respiratory protection program.
- Air monitoring.
- Radiological monitoring and contamination control.
- Radiological protection records.
- Calibration programs.

Criticality Safety. Describe the nuclear criticality safety programs developed for the operation. Include information on nuclear criticality safety evaluations, criticality safety limits, nuclear criticality safety control parameters, or other administrative or procedural controls for criticality safety.

Industrial Hygiene. Describe the industrial hygiene programs developed for the operation. The

following topics should be considered in the discussion:

- The policy or program for controlling exposures to chemicals and hazardous materials.
- Industrial hygiene programs to control:
  - —Lasing media.
  - —Magnetic fields.
  - —Beryllium.
  - —Microwaves and RF.
  - —Biohazards.
  - —Known carcinogens.
  - —Hazardous chemicals.
  - —Limited egress/confined spaces.

The following aspects of industrial hygiene programs should also be considered:

- Exposure control programs.
- Bioassay or medical monitoring program.
- Air monitoring.
- Workplace monitoring.
- Records.
- Instrumentation.
- Respiratory and personal protective equipment programs.
- Calibration programs.
- Hazard communication programs.
- Hazard evaluation programs.

Industrial Safety. Describe the industrial safety programs developed for the operation. The topics should include:

- Safety policy.
- Industrial safety programs to control:
  - —Electrical hazards.
  - —Lasers.
  - —Explosives.
  - —Pressure systems.

The following aspects of industrial safety programs should also be considered:

- Exposure control programs.
- Workplace monitoring.
- Records.
- Instrumentation.
- Calibration.

Fire Protection. Describe the fire protection/prevention program for the operation. The following topics should be considered in the discussion:

- Occupancy details.
  - —Process description.
  - —Special hazards.
  - —Fire loading.
- Appropriate type of building construction.
- Exposures to or from other facilities.
- Provisions for egress.
- Property damage limitations.
- Automatic fire extinguishing systems.
- Water supply.
- Detection and alarm systems.
- Redundant protection.
- Fire department access.
- Provisions for manual firefighting.
- Protection against unacceptable program delays.
- Fire prevention program.
- Statement that improved risk criteria have been met.

Include information on fire safety training, inspections, and drills. Discuss programs to control flammable and combustible materials and spark- or flame-producing operations.

Environmental Monitoring. Discuss the environmental monitoring program developed for the operation. The following list of topics should be considered in the discussion:

- All potential facility release points.
- The monitoring method employed at each release point.
- Analytical techniques employed.
- The surveillance program outside the facility, on-site and off-site, including:
  - —Air, soil, water, vegetation, crops, milk, and meat monitoring.
  - —Monitoring and control locations.
  - —Type of materials monitored.
  - —Monitoring methods employed.

For facilities where a site-wide environmental monitoring program already exists, describe the program and any facility-specific aspects and reference appropriate documents.

3.2.3 Accident Scenarios

The purpose of describing accident scenarios is to demonstrate the need for and the expected performance of the facility safety systems under accident conditions and to define the bounding envelope of the range of credible accident consequences. The selection of accident scenarios should provide a complete and conservative picture of the expected behavior of the facility under accident conditions. The spectrum of accident scenarios must range from high-probability, low-consequence accidents to low-probability, high consequence accidents.

Included scenarios can result from natural phenomena, malfunctions of systems, operating conditions, or operator error. Consequences can range from minor impacts on operations with no injuries to severe impacts on site or off site due to breaches of confinement systems. Sufficient detail must be included to allow reproduction of any calculation or an independent determination of the results.

While the design of a facility may require the development of a large number of accident scenarios, those documented in the SAR are only those that sufficiently define the bounding envelope of likelihood and consequence. The concept of a bounding envelope

implies that any accident experienced at the facility would have consequences less than any of those described in the accident scenarios forming the bounding envelope. Bounding scenarios must therefore be developed using conservative assumptions that are physically realizable.

For each bounding scenario include the information described in the sub-sections below.

Details. Trace the sequence of events from the initial unwanted transfer of energy to the realization of consequences. Consider the effects on workers, other on-site personnel, on-site facilities, and off-site people, property, and the environment. The discussion should show the extent to which protective systems must function, the effect of failure of protective systems, and the credit taken for engineered safety features (ESFs) during the entire course of the event analyzed. Include in the discussion the extent of system interdependence contributing (directly or indirectly) to controlling or mitigating the accident. The actions required of operating personnel should also be discussed at the appropriate place in the sequence of events.

Source Terms. The common meaning of "source term" is the amount of hazardous material available for release after applying the release fraction from primary confinement. A source term in this case is the amount of hazardous material released from the primary confinement in dispersible form. For some DOE operations "source term" may also mean the amount of energy that causes damage to a target (for example, explosive energy equivalent to 100 tons of TNT or 100 rads per second of gamma radiation). Proper documentation of the source terms includes not only the source terms but also energy sources and energy released, release fractions of hazardous materials, reduction and removal factors, and release duration.

Clearly state the assumptions made and the source of the data used in determining the source terms. To the extent possible, discuss the uncertainties connected with the calculation of source terms (for example, those uncertainties associated with equipment response time and instrumentation energy response characterisitics).

Consequences. Documentation of consequences includes not only the quantified impacts to people and property, but also the models, assumptions, and data used in the calculations to estimate the consequences. It is also important to discuss the margin of protection provided by whatever systems are depended upon to limit the magnitude of the consequences. (Thus, the margin of protection is the same as the effectiveness of the mitigators.) For the dispersion of toxic materials, include the following information in the meteorological analysis and dispersion:

- Dispersion model used.
- Dispersion parameters / stability classification and probability.
- Release effects including:
  —Plume rise.
  —Stack and building wake effects.
- Dispersion effects including:
  —Radioactive decay.
  —Inversion lid.
  —Fumigation.
  —Terrain.
  —Dry deposition.
  —Wet deposition.

For radiological-impact calculations include:

- Inhalation dose calculation parameters.
- Ingestion dose calculation parameters.
- Direct irradiation from cloud immersion or ground deposit.
- Other pathways.

Radiological dose commitments should be presented in 50-year CEDEs; in addition, identify any significant individual organ dose. Consequences from hazardous nonradioactive materials can be presented in concentrations and as multiples or fractions of Threshold Limit Values (TLVs), Permissible Exposure Limits (PELs), Short-Term Exposure Limits (STELs), Immediately Dangerous to Life or Health (IDLH) Levels, or Emergency Response Planning Guidelines. The preceding parameters should be used with caution. To insure their appropriateness, consult the Health Physics Group or Industrial Hygiene Group of the H&S Division through the Safety Team Leader.

Likelihood. Associated with any bounding scenario is the likelihood of experiencing that scenario and the associated consequences. Include the likelihood of:

- Experiencing the initiating event.
- The sequence of events occurring as described.
- The consequences occurring as estimated.

In discussing the likelihood of the sequence of events, describe the reliability of the controls that affect the sequence of events. In discussing the likelihood of the consequences, describe the reliability of the mitigators. Likelihood estimates should state any uncertainties involved. Any assumptions and data or sources of data used to estimate the likelihoods should also be included.

3.2.4 Emergency Planning

Discuss the organization and responsibility for emergency planning, the responsibility for coordination with the site emergency plan or other appropriate plans, such as state or local emergency plans, and the responsibility for approval of the emergency plans. Include an organization chart if it supports the text. Also include a discussion of the review of emergency plans, conduct of drills, and drill follow-up.

Discuss the plans developed to cope with emergencies at the facility, including discussions of inter-

faces with off-site organizations, equipment provided to respond to emergencies, communication requirements, emergency plan drills, evacuation routes, and assembly points. Describe how the emergency plans assist in the mitigation of the accident consequences described in the accident analysis. Where an emergency plan already exists, the information should reference existing documentation and identify changes. Interfaces with other plans should be identified.

3.3 Safety Analysis Approach

Safety analyses can be performed in many ways. Regardless of which specific method is used, a logical flow must be established from hazard identification to risk assessment. The basic activities are: review the operation, identify hazards, analyze hazards, determine risk acceptability, and establish controls as needed. By its nature, safety analysis is an iterative process that depends on design; thus, the tasks are not necessarily performed in order or just once.

3.3.1 Review Operation

This phase defines the scope of the analysis. Part of the work is done in the PHA and determining the hazard classification. Information can be obtained from: existing project, safety, and environmental documents; design drawings and reviews; test plans and studies; facility walk-throughs, and equipment data, if applicable; and interviews with system or process experts.

3.3.2 Identify Hazards

As with the research phase, some of the hazard identification will be done during the PHA. Hazards are identified early in the project from lists of energy sources and materials. Usually at this early stage, not enough information is available about equipment, process, or operating parameters to analyze the risks or the adequacy of controls. To return to the example in Section 3.1.1, the facility that performs nondestructive testing on welded cans containing radioactive materials, the first attempt at hazard identification might look like Table 3-2, where the basic hazards are marked from a list of energy sources. Note that the tables presented here are not meant to be comprehensive, just to demonstrate an approach to performing safety analysis.

As more becomes known about the design, these basic hazards can be characterized as to causes, occurrence probability, preventive and mitigative features, and consequences. The consequences should be assessed with and without credit for safety features. This information is usually summarized in tabular form. An example for some hazards associated with the test facility mentioned above is given in Table 3-3. (The probability terminology will be defined in Section 3.4.) Visual aids can further specify the location within the facility where the events might occur. From this information, the hazards can be analyzed in greater detail.

3.3.3 Analyze Hazards

In this step, scenarios that can result in adverse consequences are developed and analyzed. The hazard of a room fire caused by ignition of combustibles (see Event E-1 from Table 3-3) is not enough to determine the risk of adverse consequences or the controls to reduce risk. Thus, the causal factors (equipment failures, human error, loss of power, etc.) and their sequence must be determined, and the risk factors (occurrence likelihood and consequences) must be assessed. With this information management can decide whether the sequence is frequent or severe enough to represent an unacceptable risk. But first the complete list of hazards needs to be reduced to those that warrant such a detailed analysis.

Some events are excluded from further analysis: sabotage, terrorism, and events considered to be "incredible," i.e., those with a mean frequency of occurrence of 10^{-6} / yr or less. The example in Table 3-3 shows no "incredible" events.

Note: Incredible events should be analyzed in enough detail to support that conclusion.

Hazards can also be classified as to operating condition.[2] These definitions can be used to decide which hazards require detailed analysis.

Operating Condition	Description
I	Normal facility operation
II	Abnormal or off-normal (minor incidents and upsets)
III	Accidents (more severe incidents)
IV	Design Basis Accidents (limiting, requiring design consideration)

Generally, operating conditions I and II need not receive the same attention as III and IV, depending on scenario frequency. In the example in Table 3-3, the hazards may be characterized as:

Event	Operating Condition
E-1	III or IV
E-2	II
E-3	II
E-4	II or III
E-5	I
E-6	II or IV

Table 3-2. Example hazard identification.

Electrical Sources
- Capacitors
- Transformers
- Batteries
- Exposed conductors
- Static electricity
- *Other high-voltage sources

Motion Sources
- **Pulley, belts, gears*
- Shears, sharp edges, pinch points
- **Vehicles*
- Mass in motion

Gravity-Mass Source
- **Falling*
- **Falling objects*
- **Lifting*
- **Tripping, slipping*
- **Earthquakes*

Pressure Sources
- Confined gases
- Explosives
- Noise
- Chemical reactions
- Stressed mechanical systems

Cold Sources
- Cryogenic materials
- Ice, snow, wind, rain

Chemical Sources
- Toxic materials
- Reactive materials
- Pathogenic materials (virus, bacteria, etc.)
- Oxygen deficiency
- Carcinogenic material

Heat Sources
- **Electrical*
- Steam
- **Flames*
- Solar
- **Friction*
- Chemical reactions
- Spontaneous combustion

Radiant Sources
- Intense light
- Lasers
- Ultraviolet
- **X rays and ionizing radiation*
- Infrared sources
- Electron beams
- Magnetic fields
- RF fields
- **Nuclear criticality*

** Hazards present in example (non-destructive analysis facility)*

Event E-5 is an unavoidable operating hazard and is controlled by monitoring, and shielding standards and programs. Most likely, these controls will be sufficient without requiring special features. Events E-2 and E-3 are not normal operating hazards, but are likely to occur, resulting in local consequences. These are usually controlled by personnel training and industry and government standards. Events E-1 and E-6 can have severe on-site or off-site impact and may even be DBAs.

Normal operating hazards such as E-5 should have a consequence evaluation to ensure compliance with applicable standards. In the case of the non-destructive analysis facility, operational doses should be estimated to ensure that expected operational exposures comply with the LLNL ALARA Program. Events E-1 and E-6 should be analyzed to determine causal factors and their sequence, and estimates made of their expected frequency and consequence. And events such as E-3 and E-4 should be analyzed to determine if E-1 and E-6 are the bounding events. Normally, operating hazards, *some* off-normal incidents, and the bounding accidents or DBAs are presented in the SAR.

All credible accidents are evaluated to establish the need for design features and to comply with siting criteria.[3] DBAs represent the postulated accidents and conditions against which the structure, systems, and equipment must meet functional goals. DBA classes include[3]:

Operational — Explosions, fires, nuclear criticality, leak to atmosphere, and leak to aquatic environment.

Table 3-3. Example hazard characterization.

			Postulated Event Occurrence							
Event Number	Postulated Event Description	Causes	Prevention Features		Probability of Occurrence	Method of Detection	Mitigation Features		Consequences	
			Design	Administrative			Design	Administrative	Impact on Other Systems	Health & Safety
E-1	Room or equipment fire	Electrical short; ignition of combustibles; operator error; improper major maintenance operations	NFPA construction; NEC standard compliance; physical welded barriers for radioactive materials	Enforce restrictions on ignition sources and combustible materials	Medium	Visual; smell; fire dectection system alarm	Fire suppression wet sprinklers; sealed wall penetrations; fire extinguisher available; two-hr. rated fire separation between areas; manual fire fighting capability; fusible-link fire dampers; emergency exits	Evacuation of area; reentry with appropriate protective equipment for recovery; emergency plan for recovery method in place; personnel trained in use of hand fire extinguishers; fire department response; emergency team responds; on-site medical treatment available	Potential for barrier failure; shutdown of affected area operations; water damage to other equipment in area.	None to potential for burns; potential for smoke inhalation, airborne contamination and release
E-2	Electrical shock	Electrical short; wiring failures; equipment failures; improper maintenance	UBC, NEC and NFPA installations; circuit breakers; grounded conduits	Mantenance check out before turnover, experienced and trained maintenance personnel; maintenance and operating procedures; Preventive maintenance	High	Visual; audible; circuit breaker trip; local loss of power	Over current protection by circuit breakers	Operating personnel receive emergency response training; fire department trained for electrical fire control; on-site medical treatment available	Damage to wiring; local fire (see E-1); shutdown of affected area operations for repair	None to burns. Potential for severe electrical shock
E-3	Dropping of a load; pinch or crush	Operator error; overload of machine; impact with other objects during lift; lifting equipment control failure	Design of lifting devices and fixtures comply with ME Dept Design Safety Standards Manual and Health and Safety Manual requirements. Safety factors used in equipment design	Maintenance in accordance with H & S Manual; operators trained in use and limits of devices; operating procedures for performing lifting; OSPs and Safety Notes	Medium	Visual; audible	Ventilation system with two stages of HEPA filtration	Medical assistance on site	Loss of load or lifting device; shutdown of affected area operations for repair	None to potential operator injury and/or internal deposition of dispersed radioactive material.
E-4	Exposure of personnel to airborne radionuclides	Loss of containment barriers	High room airflow rate; ceiling to floor airflow; contamination survey instruments provided in key locations.	Periodic contamination surveys	Low to extremely low	Audible; CAM alarm annunciation	Ventilation system operation with two stages of HEPA filtration; contamination survey instruments provided in key locations; CAMs installed to provide alarm annunciation	Respiratory protection program in place.	Potential loss of area processes during decontamination actions	None to potential for internal deposition
E-5	Exposure to penetrating radiation	Handling of cans containing radioactive materials; operator negligence or error in material handling	Design accommodates portable shielding installation if necessary	Operators are trained in radiation safety and ALARA; operators are trained to pre-plan operations to maximize handling operation efficiency and minimize time	High	Personnel dosimetry results; health physics monitoring of operating areas; monitoring instrument and alarm	None	Health physics action level requirements for dose accumulation; DOE and LLNL requirements limit operator doses to specified levels; modify operations to reduce personnel dose	Revising operating procedures	None if doses are maintained below limits
E-6	Earthquake	Natural Phenomena	None	None	Low; extremely low for radionuclide release	Noticeable ground movement	Building structure seismically qualified	Implementation of QA program; LLNL seismic safety program; medical, and fire department responses on site; emergency plan in place provides guidance in determining responses and responsibilities for actions; personnel evacuate facilities; personnel trained for emergency response	Potential for barrier failure; shutdown of all operations for recovery	Injuries; potential for airborne contamination, and release.

Natural Phenomena	Earthquake, tornado, and extreme wind.
External Origin	Nearby facilities or operations, e.g., aircraft.

In particular, DBAs determine facility and operation design criteria. DBA analysis determines the need during design for ESFs and other controls, and to justify siting requirements.

Causal factors can be identified by using several techniques including Fault Tree Analysis (FTA), Event Tree Analysis (ETA), and Failure Modes, Effects, and Criticality Analysis (FMECA). Appendix C of this Supplement summarizes some of these techniques. The causal factors are the basic events or combinations of events that contribute to the occurrence of the scenario being analyzed. Causal factors include equipment, administrative, and human failures and operational or environmental conditions. Some questions whose answers can help identify causal factors are:

- What system, subsystem, component, process, human, environment, or other upsets or events (singly or in combination) can contribute to achieving the consequence?
- What failures and what success events contribute?
- What events contribute by duration or have a common cause?
- What pre-existing conditions contribute?

Human error considerations include:

- Hardware can be used incorrectly.
- Personnel can take shortcuts.
- Equipment can suffer from lack of maintenance.
- Training can be forgotten.
- Procedures can be ignored.
- Personnel can be affected by stress, fatigue, illness, etc.
- People can have varying levels of experience.

Table 3-4. Probability rating levels.

Probability level			
Category	**Symbol**	**Description**	**Estimated range of occurrence rate per year**
Incredible	A	Probability of occurrence is so small that a reasonable scenario is not conceivable. These events are not considered in design or SAR accident analysis	$< 10^{-6}$
Extremely Low	B	Probability of occurrence is extremely unlikely or event is not expected to occur during the life of the facility or operation. Events are limiting faults considered in design (Design Basis Accidents)	10^{-6} to 10^{-4}
Low	C	Probability of occurrence is unlikely, or event is not expected to occur but may occur during the life of the facility or operation.	$> 10^{-4}$ to 10^{-2}
Medium	D	Event is likely to occur during the facility or operation lifetime.	$> 10^{-2}$ to 10^{-1}
High	E	Event is likely to occur several times during the facility or operation lifetime.	$>10^{-1}$

3.3.4 Determine Risk Acceptability

Now that the scenario has been developed, risk factors should be applied to determine the event-sequence likelihood and severity. The estimates can be qualitative or quantitative, depending on technique and data availability. These estimates are based on engineering experience, operating history, and calculations. Most techniques provide estimates of event and scenario likelihood. Consequence estimates are made by generating source terms and dispersion patterns, usually on computer codes designed to prepare these estimates. Techniques are discussed in Section 3.4 and Appendix B of this Supplement.

The risk factors can then be compared to qualitative or quantitative criteria. Examples are discussed in Section 3.5, below. The comparison provides a basis for a management decision on risk acceptability. If the risk is not acceptable, additional barriers and controls are imposed, and the scenario analyzed again until the risk is acceptable.

Subjective guidance on risk definition and acceptability is available. This guidance rates probability and consequence (Tables 3-4 and 3-5) and risk from a matrix (Fig. 3-1). The probability and consequence levels have been defined to be consistent with: (a) hazard class definitions, (b) not assessing incredible accidents or accidents with consequences beyond design basis. Thus, the risk diagonal blocks on Fig. 3-1 (i.e., 1B, 2C, 3D, and 4E) roughly coincide with the guidelines for Operating Conditions IV, III, II, and I, respectively.[2] A detailed definition of the operating condition guidelines is shown in Table 3-6. The diagonal line, then, should represent the upper bound of what risks are "acceptable." This rating method should make review and approval easier to obtain, since it provides a logical, consistent approach to ranking risks.

Table 3-5. Consequence rating levels.

Consequence level	Description words	Maximum consequence
1	High	Serious impact on site or off site. May cause death or loss of the facility / operation. Major impact on the environment.
2	Medium	Major impact on site and or minor impact off site. May cause severe injury or severe occupational illness to personnel or major damage to a facility / operation or minor impact on the environment. Capable of returning to operation.
3	Low	Minor on site with no off site impact. May cause minor injury or minor occupational illness, or minor impact on the environment.
4	Extremely Low	Will not result in a significant injury or occupational illness, or provide a significant impact on the environment.

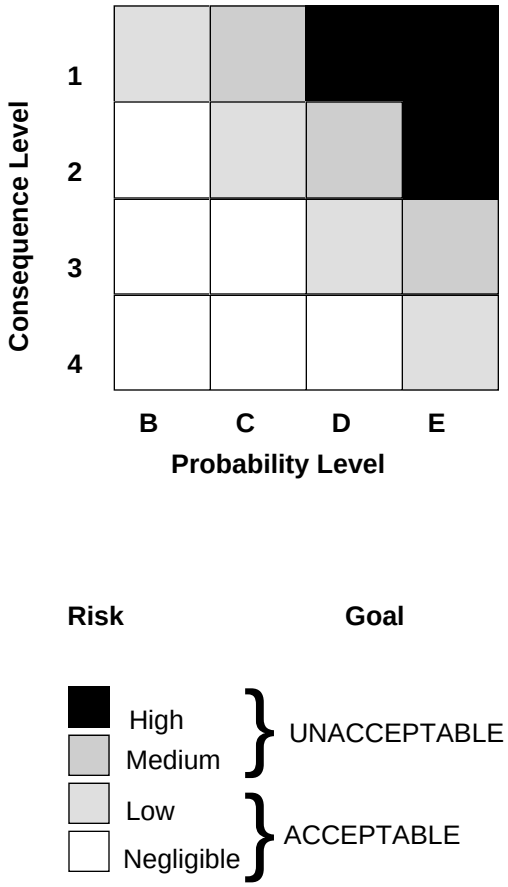


Figure 3-1. Risk matrix.

Table 3-6. Summary of general safety guidelines for nuclear facility operation.2

3.3.5 Establish Controls

The analysis will usually generate a large list of potential contributing events or event combinations. To control all of these would be expensive and inefficient, since not all events or combinations of events contribute equally to the occurrence frequency. Only those events or combinations of events that significantly contribute—and can be effectively and efficiently controlled—should be studied first.

There are three general options: eliminate the hazard, reduce the likelihood, or mitigate the consequences. The second method is usually chosen, reducing the likelihood by adding additional controls that require more failures for the event sequence to happen. These and other factors in developing controls to reduce risk are shown in Fig. 3-2. Where controls should be applied is determined from the previous analysis and considerations such as feasibility and cost. Generally, those sets with the fewest number of events, and the most likely events, will be candidates. Usually, event likelihood decreases from human error, to active equipment failure, to passive barrier failure.

Note, changing the risk of one hazard or event set may change another, and will change the individual contribution. And adding control equipment or human activities may even introduce a different hazard. Thus, interactions must be considered.

Function, location, type, and number should be considered when choosing controls (Fig. 3-2). The preference is from the top down. Thus, the controls most effective in reducing risk factors will prevent

Table 3-6. Summary of general safety guidelines for nuclear facility operation.[2]

event occurrence, be placed at the hazard source, be a design feature, and provide redundant protection. For a criticality hazard, risk determination and control application requirements are specified in DOE Order 5480.5. The design of these controls is also specified in DOE Order 6430.1A.

The controls should be reviewed to see if they are sufficient and reasonable, and their response to upset conditions should be determined. Controls are defined as sufficient if the risk factors are acceptable, and they are reasonable if they are cost effective and operationally feasible. Further, a safety control function differs from a normal operation function, since it is designed to maintain its safety function and level of risk reduction during accident conditions—thus, it must be reliable and effective, which may lead to other requirements such as redundancy and emergency power.

Controls for which credit is taken should be listed in the analysis portions of the report. Specifically, list the facility safety systems that are used to preclude the scenario from occurring or to mitigate the effects of the scenario if it does occur.

3.4 Likelihood

One risk factor is the likelihood of the postulated scenario, or how often the adverse consequence is expected to occur. The likelihood can be estimated in absolute terms (probability) or as a recurrence rate (number of events per year). These estimates can be quantitative or qualitative. Either way, the data for the estimates come from sources including engineering judgment, historical evidence, Reliability and Maintainability analyses, and equipment failure rate databases. **Note**: *the confidence level for this data varies widely and should be considered when reporting numerical values.*

3.4.1 Basic Events

Historical evidence can be obtained from several sources including: incident reports, Unusual Occurrence Reports (UORs), Atomic Energy Commission Serious Accident bulletins, the DOE course "Prevention of Significant Nuclear Events," the LLNL Fire Department, and the DOE reportable incident computer database at the System Safety Development Center (SSDC), EG&G Idaho. The Safety Services Division of the HC Department has access to historical evidence databases. Some of this information may not apply to the situation being analyzed, so take care to ensure accuracy and conservatism. Failure rate estimates can be obtained from existing databases or reports, including:

- Non-Electronic Parts Reliability Data, NPRD-2, Rome Air Development Center, 1981.
- Summary of Component Failures in Nuclear Power Plants, NPRD-Q04, 1985.
- IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power-Generating Stations (ANSI/IEEE Std. 500), John Wiley and Sons, 1984.
- Reliability Engineering and Risk Assessment, E. Henley and H. Kumamoto, Prentice-Hall, 1981.
- Generic Data Base for Data and Models Chapter of the National Reliability Evaluation Program (NREP) Guide, A. J. Oswald, et al., EG&G Idaho, EGG-EA-5887, June 1982.
- Military Handbook Reliability Prediction of Electronic Equipment, MIL-HDBK-2170, 1982.
- *Reactor Safety Study—An Assessment of Accident Risk in U.S. Commercial Nuclear Power Plants*, U.S. Nuclear Regulatory Commission, WASH–1400 (NUREG-75/014) October, 1975.
- *Component Failure-Rate Data with Potential Applicability to the Hot Experimental Facility*, OPST-CFRP-80-113, SRL, 1980.
- *Component Failure-Rate Data with Potential Applicability to a Nuclear Fuel Reprocessing Plant*, DP-1633, SRL, 1982.

Some of this information is available from the HC safety analysis advisors.

The database list above is not meant to be all inclusive or to be used without determining whether the data is even applicable. In fact, the list raises several issues. One is that most of the data were generated for military systems or the nuclear power industry where there is a long history of equipment reliability. At LLNL most operations involve short-term experiments, technology demonstrations, or unique equipment, so existing reliability data may not apply. Also, even if standard equipment is used that is in a database, it may have been modified, especially if failures have occurred. However, existing information can be used to determine a probability *range* from failures of similar systems.

Other information can be found in failure studies and safety analyses for existing facilities or operations (at LLNL or other DOE sites) that have already been verified or approved. Again, take care to assure the applicability and consistency of this information.

Quantification is even less valid for human error. Techniques are available for estimating human error rates, but few people are skilled in these methods, and the base information may not be applicable for LLNL operations. Quantification may still be used—in fact, without some quantification, risk acceptability is difficult to establish—but a poor quality assessment is of no real value and may be non-conservative and misleading.

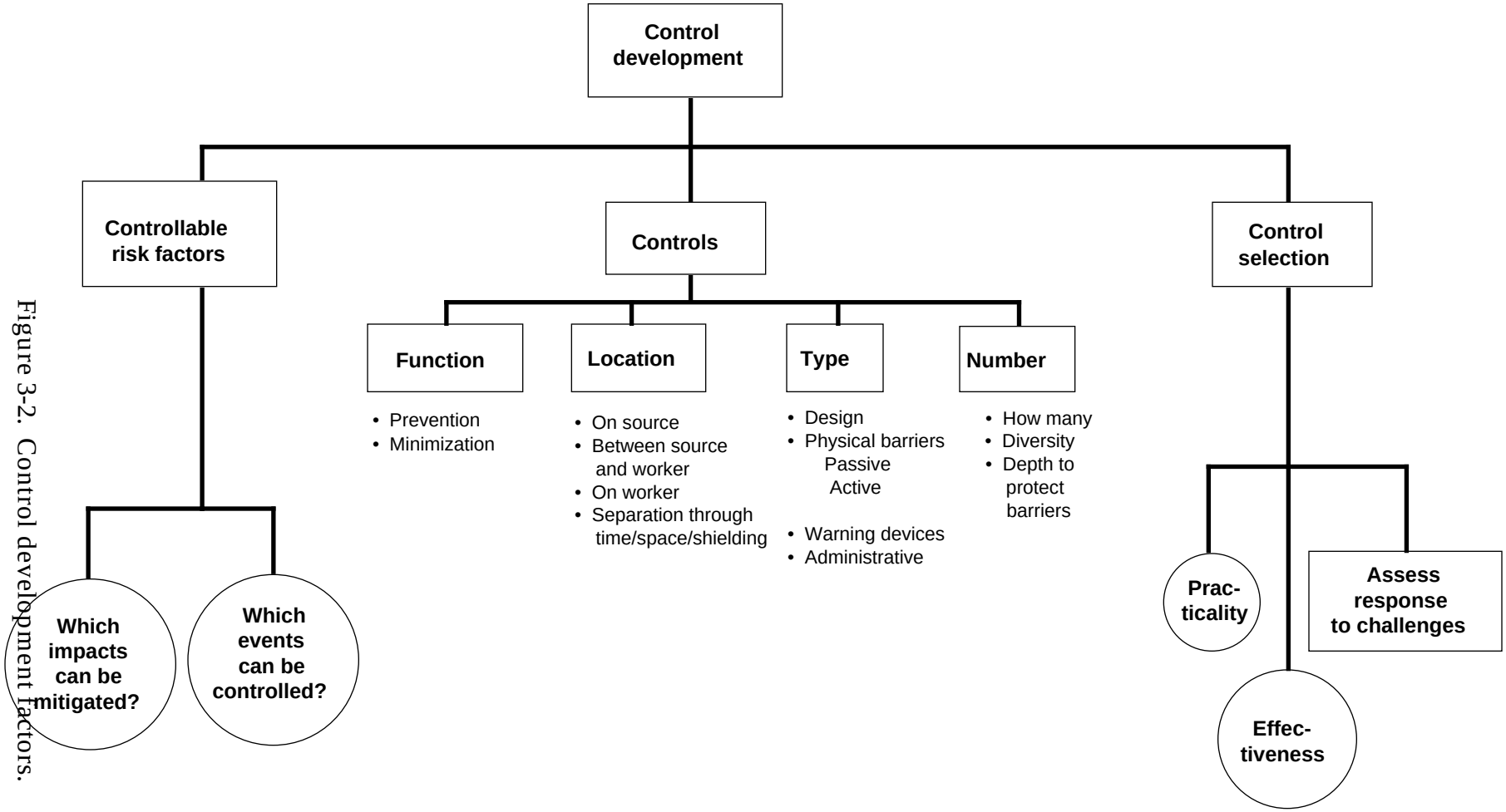


Figure 3-2. Control development factors.

Figure 3-2. Control development factors

3.4.2 Scenario

The scenario is the description of how the assessed accident takes place, the combinations of basic events (conditions and failures) that, if they occur, will cause the accident and result in adverse consequences to the public, workers, environment, or operation. One way of categorizing accidents is as follows:

Operational (internal)	Explosion or uncontrolled reaction
	Fire
	Criticality
	Leaks
Natural phenomena	Flood
	Earthquake
	High wind or tornado
External origin	Credible aircraft impact
	Credible accidents from other nearby facilities or operations

This list is not complete, nor is it the only way to group scenarios.

Combining the likelihood of basic events will produce an estimate on how often the analyzed scenario may occur. The choice of subject being analyzed, contributing events, and the relationship of those basic events is extremely important. The logic must be accurate and supportable, as it will directly affect the conclusions of the safety analysis. If the chosen model does not represent reality, neither will the result.

Several logic models can be used to estimate combined likelihoods. These include Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Probabilistic Risk Analysis (PRA), and various statistical models. This Supplement will not discuss in detail nor recommend any particular approach. The choice depends on several factors and is best left to the particular analyst and situation involved. Some analysis techniques are summarized in Appendix C.

FTA is a "failure" model that defines an accident scenario in terms of basic failures and the relationship between these events. The result is a collection of "sets" or failure combinations that, if they occur, will produce the undesired consequence. These sets are useful to identify where to expend resources to reduce the likelihood of an accident.

A simple, qualitative shortcut would be to focus on those sets from an FTA with fewer basic events. An advantage is this provides a fast, less-expensive analysis of problem areas. A disadvantage is that if the analysis stops with identification of the "sets," that important information (i.e., common-cause interactions) may be lost.

FTA is widely used. There are several courses on, and computer codes for, developing and quantifying fault trees. Because this method analyzes how accidents develop, FTA concentrates on prevention rather than mitigation. FTA does not provide a range of consequences, to determine consequence ranges, event trees can be useful.

ETA can determine the range of consequences resulting from a specific failure. An initiating event is postulated and then the sequence of events (both success and failure) that follow is described. The branch points are commonly called lines of assurance and represent mitigative features that can reduce the event consequence. Thus, event trees are useful in determining safety system response. Event trees can be combined with fault trees by adding safety system failure modes. Sometimes this is called a cause-consequence diagram. Event trees can be useful in assessing natural phenomena. Because both success and failure modes are considered, a range of consequences can be estimated. Probabilities can be added by quantifying the likelihood of success or failure at each branch point. This approach can be time consuming.

PRA is a special type of analysis that has come into prominence in the nuclear power industry. The technique is exhaustive, expensive, and requires experience. The decision to use PRA should be carefully considered.

3.5 Consequence

Next, the consequences are assessed. Consequences are usually split into radiological and non-radiological categories. Non-radiological consequences include: hazardous material releases, injuries, equipment or facility damage, and programmatic impact. Off-site and on-site effects are considered for normal and accident conditions.

3.5.1 Radiological Assessment

For nuclear facilities the radiological impact to the environment, workers, and public is considered by comparing radionuclide effluents or personnel doses to applicable guideline limits. Both on-site and off-site impact during normal and accident conditions should be assessed. Specific criteria exist for assessing the radiological impact of a nuclear facility operation, which include limits and modeling parameters. These criteria can be found in DOE 6430.1A (draft). Despite its draft status, DOE-HQ has specified the use of this Order.

Normal Operation. This portion of the safety analysis is intended to demonstrate the adequacy of the design for normal operation. Essential aspects may include: contamination control, exposure control, criti-

cality control, radiological monitoring, procedures, training, and dosimetry. The programs in place to provide for the controls are discussed, and the impact of normal operations is assessed.

For normal operation, the radiological impact assessment usually considers routine releases, if any, and worker exposure to direct radiation. The basic standards are in Chapter 33 and its supplements to the *Health & Safety Manual*.

"The effective dose equivalent to the public...shall not exceed 500 mrem / yr for occasional exposures, and 100 mrem / yr for... > 5 yrs. Radioactivity in airborne effluents...shall not result in > 25 mrem / yr to the whole body or 75 mrem / yr to any organ."

For personnel under LLNL control, "The dose limit for exposure of the whole body...shall not exceed 3 rem in any calendar quarter or 5 rem / yr...for hands, feet, and ankles shall not exceed 25 rem in any...quarter or 75 rem / yr."*

Refer to Chapter 33 of the *Health & Safety Manual* for complete discussions of these and other standards, as well as the LLNL ALARA program.

Generally, compliance is demonstrated by calculating worker and public doses and comparing these with the above standards. The results are presented in the "Normal Operation" chapter of the SAR. Information for the calculations can include:

1. Source term from normal operations (how much material and type, specific activity, time / motion task study, shielding).
2. Pathway (direct, inhalation, ingestion, which radionuclide).
3. Release parameters (fraction, concentration, stack height, normal operating meteorology).
4. "Receptor" parameters (breathing rate, distance).

Note, exposure is assumed to be continuous for normal operation releases.

For a postulated release, several computer codes are available at LLNL and outside that can be used. The applicability of the model, input data used, and calculational limits must be considered in making a choice. The Health Physics Group should be consulted through the Safety Team leader for guidance on computer codes, consequence estimation, and specific assumptions.

For exposure to direct radiation, several factors should be considered in the estimate, including material, throughput, exposure time, work location, and shielding. Figure 3-3 describes an approach that can be used to determine if the specific operation satisfies dose limits. Another way to estimate radiological impact is to compare with existing operations, provided valid information exists for the operation being analyzed. Finally, empirical studies can be performed as needed to estimate personnel doses.

Accident. *Health & Safety Manual* Supplement 33.42 states, "...design basis accidents must be evaluated to show that the maximum calculated dose does not exceed 25 rem to the whole body, 300 rem to the thyroid, 300 rem to the bone surface, or 75 rem to the lung," both on site and off site, which is a basic siting and design requirement. Other guidelines are available that may be used for comparison. Two examples are shown in Tables 3-6 and 3-7.

Some of the same codes used to estimate normal release impact may be used for accident releases, but the model and data must be consistent with accident conditions. This will affect the choice of some parameters, including exposure time, release point, and meteorology. The dose from releases depends on the source term provided to the model. The source term in turn depends on several factors including amount of material at risk, dispersion mechanism (spill, fire, oxidation, etc.), release fraction, accident duration, and if credit can be taken for HEPA filtration.

For a postulated criticality accident, the impact can be estimated by the methods in NRC Regulatory Guide (RG) 3.35, depending on the fission yield. The yield depends on critical system characteristics (material type, mass, form, amount). The potential impact of a criticality consists of direct radiation exposure to personnel and a release of radioactive materials to the environment. The Criticality Safety Group should be consulted through the Safety Team leader to estimate the possible impacts of a criticality. NRC RG 3.35 provides some guidance on estimating criticality impacts.

3.5.2 Non-Radiological Assessment

Assessment of non-radiological consequences is somewhat less precise than radiological, because past emphasis has been on radiological. DOE risk limits have not been established for non-radiological impacts.

Normal Operation. Assessments are conducted to demonstrate the adequacy of design for normal operation. The aspects for non-radiological safety include: fire protection, industrial safety, industrial hygiene, and special disciplines such as laser safety. The programs for these types of disciplines are discussed in the safety analysis, and any normal operating impacts are assessed. These impacts may include normal operating effluents and resource consumption, information on which can be obtained from Environmental Assessments or Environmental

* These limits will be changed around January 1989. They will be updated in the next revision of this Supplement.

Impact Statements.

For fire safety, assessments can include compliance with National Fire Protection Agency NFPA 101 or the "improved risk" concept of DOE Order 6430.1, and fire evaluations based on expected loadings using, for example, the FIREONE, FIRETWO codes.[4] The industrial safety section includes describing the controls and expected hazardous sources associated with pressurized systems, electrical systems, mechanized equipment, or cryogenic equipment. Industrial hygiene includes describing the hazards associated with such topics as oxygen deficiency, noise, non-ionizing electromagnetic radiation, and chemical safety. Any topic may have some technical evaluation to better define the hazard, operation, or level of controls required. Adherence to industry standards or comparison with established exposure limits can determine risk acceptability.

Accident. Non-radiological consequences can include personnel injury, hazardous material release, equipment or facility damage, and programmatic impact. Consequence levels are presented by subject in Table 3-5. Off-normal incidents (e.g., parameters outside normal operating range) should produce consequences no higher than a Consequence Level 3.

Accidents can produce higher consequences. For

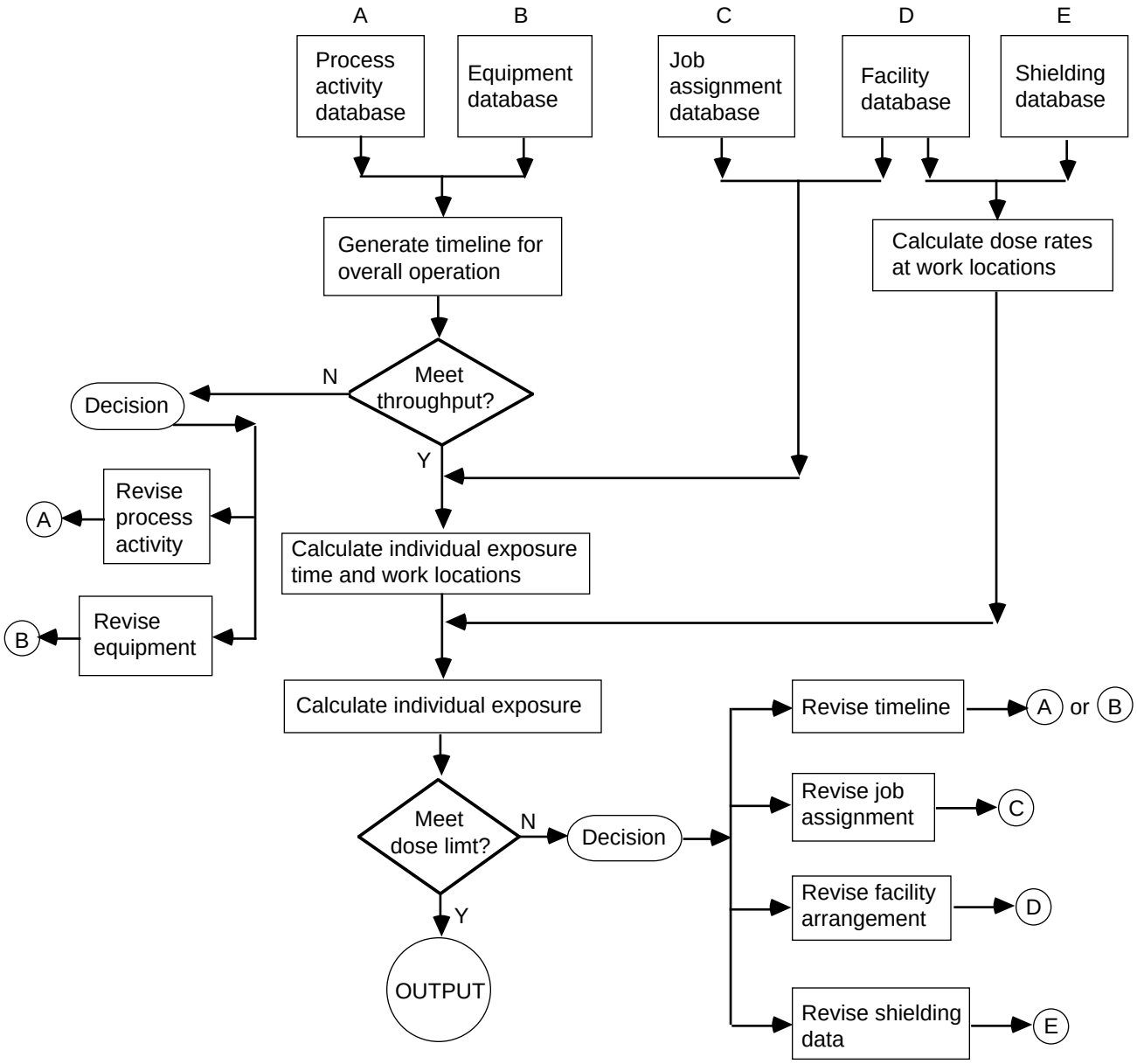


Figure 3-3. General approach for assessing worker doses.

Table 3-7. Potential radiological dose guidelines for accident evaluation.[3]

Probability range (Occurrence/yr)	Dose guideline (rem)				
	Whole body	Lungs	Thyroid	Bone surface	Other organs[a]
> 10–2	< 0.01	< 0.03	< 0.12	< 0.12	< 0.06
10–4–10–2	0.01–0.50	0.03–1.5	0.12–6	0.12–6	0.06–3
10–6–10–4	0.5–2.5	1.5–75	6–300	6–300	3–150
< 10–6	> 25	> 75	> 300	> 300	> 150

[a]Based on ICRP recommendation of weighting factors assigned to each of organs receiving highest dose equivalent (ICRP 1977).

example, a credible explosion resulting from a human error in handling materials may have death as a consequence. Since the occurrence rate is lower for accidents, the increased consequence may be acceptable. For the most part, injury, damage, and programmatic impact are hard to assess accurately. One reason is that worker and recovery team actions and response time can make the difference between minor or major consequences. The best method is to use the experience of discipline professionals from HC or incident reports from actual accidents. Some incident reports are available from the safety analysis advisors.

Hazardous material releases can be modeled. The models include smoke tests, tracer gas tests, and calculational models, which are discussed in detail in *Health & Safety Manual* Supplement 12.01. Estimates of materials in effluent streams can be compared to applicable standards and guideline values to judge acceptability. Some of these are:

- *National Primary and Secondary Ambient Air Quality Standards* (40 CFR 50).
- *National Primary and Secondary Drinking Water Regulations* (40 CFR 141 and 143).
- *EPA-EP Toxicity Limits for Liquid Discharge* (40 CFR 261).

Release estimates can also be calculated using, for example, the Complex Hazardous Air Release Model (CHARM) from Radian Corp. Note that no Environmental Protection Agency (EPA) approved model exists; EPA requires only the use of a Gaussian puff release model. CHARM is one example of a validated code.

Finally, any comparisons to determine risk acceptability should be made or reviewed by the Industrial Hygiene Group of the H&S Division.

3.6 Risk

The risk associated with an event is a function of its probability of occurrence and its consequences. The common practice of calling "risk" the product of probability and consequence is not considered sufficiently informative because both components are needed to fully describe the nature of the risk.[3] Further, to define risk as a mathematical function would require estimating all consequences and their occurrence rates, then summing the results. This is not practical or achievable for most operations with which this Supplement is concerned; in addition, unless it is carefully researched and performed, the result is likely to be misleading.

"Risk assessment" as described in this guide represents analysis of worst-case accidents, comparison of the risk factors with established criteria to determine acceptability, and analyzing other accidents to ensure that the worst-case accidents represent the bounding risks.

Risk assessment also represents the specific analysis technique (e.g., FTA, ETA, or PRA). DOE-HQ has not specified a risk-assessment method, nor has it defined specific numeric acceptable levels of risk. This Supplement discusses only local methods presently in use, both qualitative (informal) and probabilistic (formal). Some organizations within LLNL that can assist SAR preparers in applying various risk-assessment techniques are:

- The Risk Assessment and Reliability Engineering Group of the Nuclear Test Engineering Division.
- The Systems Research Group of the Engi-

neering Research Division.

From Section 3.3.4, subjective guidance on risk definition and acceptability is available. This guidance rates probability and consequence (Tables 3-4 and 3-5) and risk (Fig. 3-2). The goal is to design and operate facilities such that risks are at the lowest possible level, and DOE-SAN policy is that all operations are to be at the Low risk level.

Radiological release and nuclear criticality are two special cases. For nuclear facilities DOE-SAN assesses safety analyses based on the release impact levels in Table 3-6.[3] Also, the acceptability of nuclear criticality risk, controls, and parameters is detailed in DOE Order 5480.5 and DOE Order 6430.1A, which state, "Process designs shall incorporate sufficient safety factors so that at least two unlikely, independent, and concurrent changes in process conditions must occur before an accidental nuclear criticality is possible." This is the "double contingency" principle. Since it controls event occurrence, the scenario likelihood should be analyzed to demonstrate conformance. Double contingency should be demonstrated for design as well as verified in analysis of the accident scenarios.

3.7 Operational Safety Requirements

Operational Safety Requirements (OSRs) define the conditions, safe boundaries, and bases of such conditions, and the management or administrative controls required to assure safe operation. Thus, OSRs are of controlling importance to safety and represent those items necessary to maintain the "Safety Envelope" as specified in the SAR accident analysis. Operation outside of the OSRs will be an Unreviewed Safety Question (USQ) requiring a revision to the safety analysis. Unintentional operation outside of OSR boundaries generally requires the preparation of a UOR after the occurrence. Further, OSRs that are "fundamental operating limits" (e.g., facility mass limits, or prohibitions on incompatible material) must be clearly detailed in the safety analysis. OSRs are listed in the safety analysis, the Management Plan, and applicable FSPs or OSPs. OSRs are strictly controlled, as described in *Health & Safety Manual* Supplement 1.13.

Because of the importance of OSRs and the potential impact of changes to them, bounds should be conservatively stated while allowing, *if possible*, enough margin for operation to forestall frequent and expensive changes to the applicable safety documents.

OSRs deal with both technical and administrative concerns. Technical matters should address those features (parameters, operating conditions, systems, or components) of the facility or process that are *essential* to safety. Administrative OSRs should cover those organizational and functional requirements important to safe operation. Through analysis and evaluation, the SAR should fully develop the details of the OSR bases. Some guidelines for selecting OSRs are presented in Table 3-8. The list is not complete for specific situations —rather, it provides an idea of the types of controls that should be considered. OSR categories are:

Safety Limit/Limiting Safety System Setting. Variables directly related to performance and integrity of safety system or function. The Safety Limit (SL) is chosen such that, if it is not exceeded, no serious consequence will occur. Limiting Safety System Settings (LSSSs) are at a level to prevent inadvertent safety system operation while ensuring that upset conditions

Table 3-8. OSR selection guidelines.

Should be considered for an OSR if it—

- Prevents undesirable buildup of fissile material that could cause a criticality.
- Is a technical matter important to preventing incidents with significant hazard potential.
- Is an administrative control related to achieving and maintaining safe operation or shutdown.
- Functions as barrier to significant release.
- Functions as a warning for off-normal conditions with significant hazard potential.
- Is necessary to prevent degradation of safety system function when operation is required to maintain risk at acceptable level.

Should <u>not</u> be considered for an OSR if it—

- Is not identified as a *necessary* control in the safety analysis.
- Is not of controlling safety importance and is effectively covered by other approved requirements.
- Functions to maintain controls *well within* normal operating limits.
- Limit cannot be exceeded due to physical characteristics of the system. If an event or human activity can challenge the physical characteristic, then the limit may be an OSR.

will not exceed the SL.

Limiting Conditions for Operation. Limits that specify the lowest acceptable equipment performance level or system or component portions operable as required for safety.

Surveillance. Tests, calibrations, or inspections and frequencies needed to verify performance and availability.

Design. Design characteristics of special importance (criticality controls, shielding, containment, confinement).

Administrative. As a minimum, the controls and staff needed for safety requirements, and action to be taken in the event of OSR violation.

3.8 Design Criteria

A basic requirement of safety analyses (from DOE Order 5481.1B) is to identify and demonstrate conformance with applicable guides, codes, and standards. Any deviations are to be evaluated and documented in the report. With that in mind, the draft SAN MD 5481.1A provides guidance on content and format (Appendix B) for Chapter 4, Section 4.5 of SARs. This MD states:

> "This section should provide a summary of the design criteria for all structures, systems, and components that are important to safety. This information should identify and demonstrate conformance with applicable guides, codes, and standards. Deviations from current DOE design criteria should be evaluated. A table or chart listing the criteria, whether the criteria conforms or not, should be presented."

Basic design criteria are found in DOE Orders 5480.5 and 6430.1A, the LLNL *Health & Safety Manual*, and the *Design Safety Standards Manual.* An example of demonstrating conformance with applicable criteria is shown in Table 3-9. NOTE: This table is for conformance with DOE 6430.1 *not* 6430.1A. An example of conformance with DOE 6430.1A is not available at this time. (The entire table is not included here, just enough to summarize the technique.)

DOE Order 6430.1A was issued as a draft, but for immediate use, on January 8, 1988. This is an important document that covers a wide range of design and safety analysis requirements. This Supplement will not attempt to summarize those requirements. The reader should become familiar with DOE 6430.1A requirements as they apply to specific facilities or operations for which safety analyses will be performed. Below are *a few* requirements that control safety analyses for "Special Facilities," which includes non-reactor nuclear facilities. The requirements listed below are quoted out of context, but presented to give an idea of the subject matter covered in the DOE Order.

> "For a deterministic analysis, events considered are those judged to possibly occur based on technical review of the specific facility design and related nuclear processes or activities. Probabilistic analysis considers those events whose annual probability of occurrence exceeds 10^{-6}."

> "Unless the safety analysis can demonstrate that the risk from an aircraft crashing into the facility is acceptable, potential aircraft crashes shall be considered among the spectrum of man-made missiles that confinement structures shall be designed to withstand or against which they shall be protected."

> "The design shall ensure that a single failure does not result in the loss of capability of a safety class system to accomplish its required safety functions. To protect against single failures, the design shall include appropriate redundancy and shall consider diversity to minimize the possibility of concurrent common-mode failures of redundant items."

> "Nuclear criticality safety shall be achieved by exercising control over both the quantity and distribution of all fissile materials and other materials capable of sustaining a chain reaction, and over the quantities, distributions, and nuclear properties of all other materials with which the fissile materials and other materials capable of sustaining a chain reaction are associated. Design considerations for establishing such controls shall be mass, density, geometry, moderation, reflection, enrichment, interaction, material types, and nuclear poisons."

> "Process designs shall incorporate sufficient factors of safety so that at least two unlikely and independent concurrent changes must occur in process conditions before a criticality accident is possible."

> "Nuclear criticality safety shall be controlled, in decreasing priority, by geometric spacing, density and/or mass limitation, fixed neutron absorber, soluble neutron absorber, and administrative control. The design of the facility shall emphasize engineered safeguards and shall not rely strictly on administrative controls."

Table 3.9. Example of a Criteria Conformance Evaluation.

Table 3.9 (continued).

> "Where frequency estimates for a specific operation at a specific location shows the frequency of a criticality accident to exceed 10^{-6} per year, the combination of shielding design and facility layout shall minimize the number of potential fatalities."

In facilities where plutonium or enriched uranium is processed, additional requirements include:

> "A safety analysis under DOE direction shall establish the minimum acceptable performance requirements for the ventilation system and the response requirements of system components, instrumentation, and controls under normal operations, anticipated operational occurrences, and DBA conditions."

> "The safety analysis shall determine system requirements such as the need for redundant components, emergency power for fans, dampers, special filters, and fail-safe valve / damper positions. The safety analysis and the guidelines provided by the cognizant DOE authority shall determine the type of exhaust filtration required for any area of the facility during normal operations, anticipated operational occurrences, and DBA conditions."

H&S Division discipline professionals and appropriate Safety Team members should be consulted on the applicability of and satisfying the safety analysis requirements of DOE Order 6430.1A and 5480.5.

For those projects that require an Operational Readiness Review (ORR) prior to operation, the adequacy of the design relative to the design criteria will be addressed in the ORR as well as the completion of important SAR milestones. Details can be obtained from Quality Assurance (QA).

3.9 Cost and Schedule

This section provides guidance on safety analysis cost and schedule. The relationship between major project milestones and safety documentation for new projects was shown earlier in Fig. 2-3, and a general list of safety analysis tasks was given in Table 2-1. These indicate that safety analysis must be started early and is a vital part of project authorization to conduct operations. It is especially important to allow for a potentially long review and approval process and to identify health or safety problems in time for efficient resolution. HC's involvement during project design and construction is shown in Fig. 3-4. Note that the figure represents an ideal situation.

From Table 2-1 note that the safety analysis tasks have four general phases: estimate effort (includes determining hazard classification), perform and document analysis, review and approve, and maintain document. For moderate or high hazard class, the first three phases can take six months to two years depending on hazard type, operation complexity, project sensitivity, and the level of review and approval.

In terms of SAR chapter preparation, the sequence may be as follows:

First Ch. 1, 3, 11, 12, 14 (most of this information may already be available).

Second Ch. 4, 5, 6, 7, 8, 9 (the design descriptions and safety analysis).

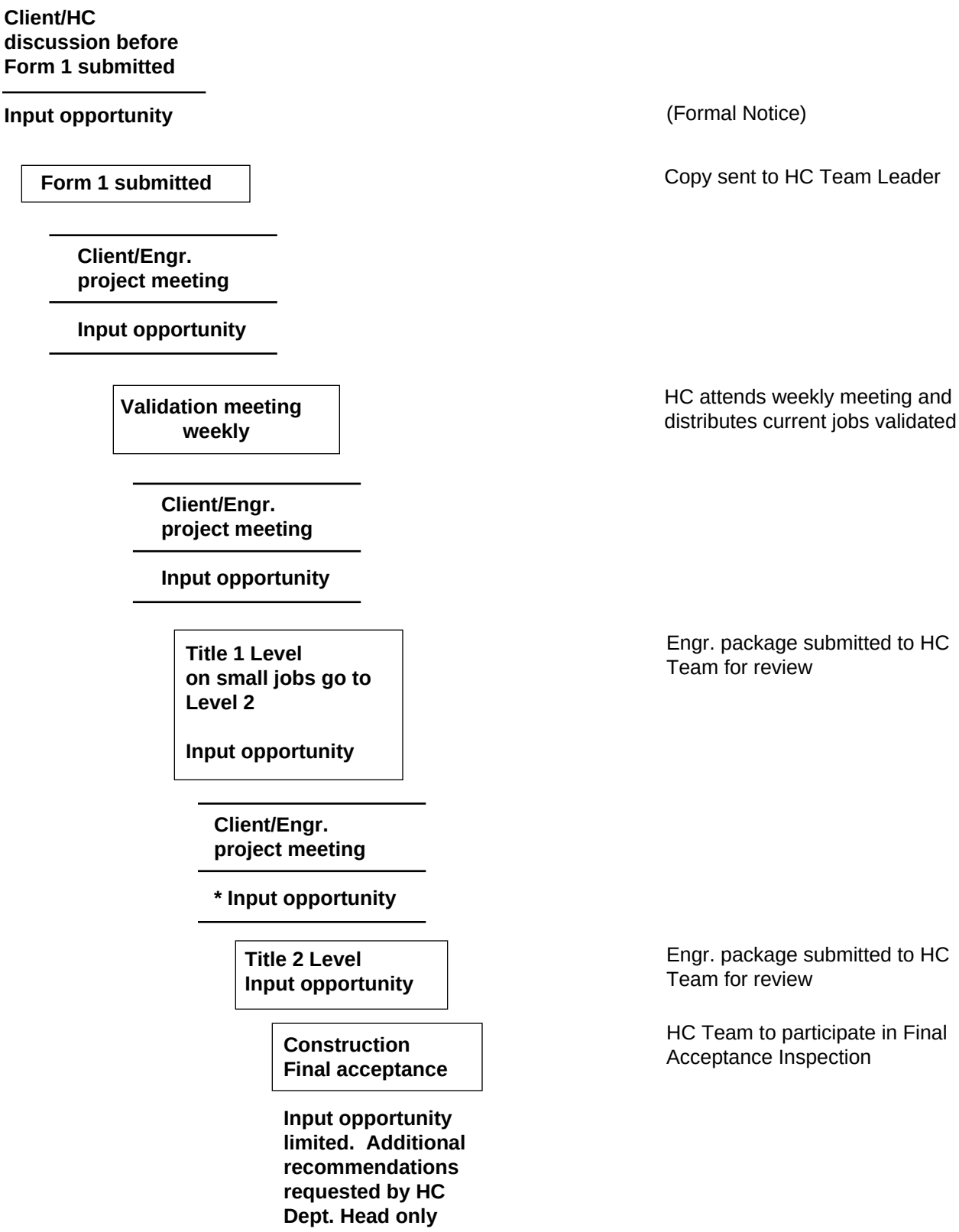
Last Ch. 2, 11, 13 (summary, OSRs, and references).

See Appendix B of this Supplement for specific chapter content. With this sequence in mind, the second phase of chapter preparation will consume the most time and effort.

For example, consider a major modification to a high hazard nuclear facility. The product is an addendum to an existing report. In other words, a separate PSAR and FSAR was not assumed. About 75% of the report is expected to be new material. Criticality and dose exposure studies are required. Development of a fire scenario will probably result in a fire loading study and an off-site dose study for radiological releases. The cost estimate detailed in Table 3-10 covers first-draft preparation through two review cycles, which will carry the safety analysis through DOE-SAN review. The effort required to prepare the SAR and obtain LLNL and DOE-SAN review and approval is, for this particular modification, 3.5 man-years. The estimate was made by reviewing similar safety analyses and interviewing personnel involved in the preparation of those analyses. The estimate does not include the impact of DOE-HQ review, which is difficult to assess because it varies considerably with personnel and politics involved. Also, it affects how the analysis is performed and how the document is prepared initially. The total cost could be as much as twice the above estimate. Certainly, the safety analysis effort for Building 332 supports this assertion.

A recent estimate was made for a SAR for a moderate hazard nuclear facility whose operation was easier to analyze (no criticality scenario would be involved). The operations were also less complicated. For hazard classification through DOE-SAN approval, an estimate of about two man-years was made. DOE-HQ review was not included.

Rough estimates can also be made using some simple assumptions: A well-defined, detailed technical analysis resulting in a moderate-to-large document



* Attendance by HC at client/engineering meetings will be determined by size and scope of job and may not be held on all projects.

Figure 3-4. Notice to Hazards Control of engineering projects.

with a formal review can cost $1000–2000 per final page of new material, plus a lesser cost for incorporating or modifying existing material. Also, for the same class of document (e.g., the SAR for a nuclear facility), the cost can be about 2–3% of the total project cost. The first two safety analysis phases are the most labor-intensive and thus are the most expensive.

For large, costly projects, the cost of safety analysis can be considerable when compared with past requirements—however, a few percent of the total cost is not a significant fraction. Also, while extra safety considerations in design may be more expensive up front, it should reduce operating costs later, and it will reduce the potential for recovery costs or impact of downtime by reducing the potential for occurrence of an incident.

Note, safety analysis is an iterative process. Significant changes in design will affect the cost and scheduling of a safety analysis. To minimize the impact of these changes, the safety analysis team should be apprised of changes as soon as possible when they become a part of the design requirements.

3.10 Other Considerations

3.10.1 Analysis Considerations

Any safety analysis must be comprehensive, consistent, logical, and have adequate support. Presenting one bounding accident is only a part of the complete analysis. Sufficient support should also be provided to prove that other accidents were not overlooked or not sufficiently analyzed. Other recent approved safety

Table 3-10. Cost estimate example of a modification to a nuclear facility.

Task	Pages	Estimate (man-hours)		
Management		480		
Criticality / dose study		800		
Fire study		160		
Release / dose study		160		
Miscellaneous studies		200		
Preparation		Draft	Rev. 1	Rev. 2
Introduction, summary, site characteristics	60	120	40	20
Design criteria and descriptions	120	500	250	125
Radiological protection and accident analysis	120	500	250	125
Conduct of operations, OSRs, other	40	120	40	20
Appendices	100	240	120	60
Editing, document preparation, word processing	440	240	210	60
Total (includes a 33% contingency)		Approximately 3.5 man-years.		

analyses should be researched to determine what is acceptable and to provide a consistent basis for the analysis being performed. However, using the same accidents as other analyses may not be sufficient without additional work to ensure that they apply and represent the project being analyzed. Other topics to consider are:

- Non-radiological impact (sometimes the radiological impact is analyzed in great detail and non-radiological hardly at all).
- Extrinsic accidents (the impact on other facilities or projects and vice versa—or credible airplane crashes).

Providing enough support is important. Do not require a reviewer to make large intuitive leaps. On the other hand, do not overdo the report since the intent is to document only *safety* design, analysis, and conclusions.

Qualitative analysis is usually performed instead of quantitative analysis, for reasons including excessive cost, inapplicability or unsupportability of numbers, or lack of personnel trained in qualitative techniques. As a minimum, ranges of likelihood and consequence should be estimated to demonstrate conformance with the risk matrix presented earlier. Further, the worst-case accident in each likelihood class and accident category should be assessed as a minimum and their risks compared to the suggested guidance in Section 3.3.4. Addressing only minimum requirements or presenting only minimum results may not satisfy the intent of safety analysis objectives.

Safety analysis rules are different from other engineering approaches. If a system or component is exposed to conditions beyond design, the system is assumed to fail. This also applies if the safety function depends on a lower rated system that may fail. Thus, credit is taken only for controls that maintain their safety function when subjected to accident conditions. This is another reason for early analysis during design. Safety features are better if they are designed-in rather than added on, are physical rather than administrative, and prevent rather than mitigate.

The impact on other facilities from releases should also be analyzed. In particular stack height and ventilation parameters can be major factors in determining worker and public exposure estimates. Other factors are building location and building wake effects. Some information on stack effects is given in *Health & Safety Manual* Supplement 1.04. Consult with the Industrial Safety Group of the H&S Division for additional information.

3.10.2 Relationship with NEPA Documents

The National Environmental Policy Act (NEPA) requires the preparation of an Environmental Impact Statement (EIS) for major Federal actions that may have a significant environmental impact. The EIS is usually completed before beginning significant detailed design. The safety analysis required by DOE 5481.1B naturally follows the EIS. It permits an evaluation of whether the design will meet performance assumptions made in the EIS, thereby providing the first level of assurance that environmental protection will be as intended.

Recent accident descriptions in EISs have included assessments of accident scenarios whose occurrence would fall below 10^{-6}/yr. These scenarios are beyond design basis and represent "maximum" accidents where credit for mitigative features is questionable and all material is presumed to be at risk.

Accident analyses should be consistent within the various reports. However, one purpose of the SAR is to assess credible risks and the adequacy of safety features and to determine risk acceptability through DOE and operating contractor approval. Thus, the maximum accident has no place in risk assessment for safety analysis purposes.

3.10.3 Team Considerations

The safety analysis preparation team should be composed of project and safety discipline personnel; some members should have a background in performing safety analysis. Team interfaces should be cohesive and constructive rather than adversarial. A goal, schedule, and analytical reviews are needed—but insufficient support, nonconstructive and continual reviews or redirections, or restraining communication will not result in a high-quality, meaningful or cost-effective document.

Team personnel must also demonstrate an open-mindedness in approach by becoming familiar with the design, operation, and basic purpose of the project. These suggestions apply to the review process and review personnel as well as to document preparation.

3.10.4 Review Considerations

The purpose of a SAR review is to document the adequacy of preventive or mitigative design features and administrative controls to limit risk, as well as to provide a basis for project-phase authorization through proper approvals. Since a cursory review may only postpone problems (to a time when resolution may be more costly and difficult), reviewers should be provided with sufficient time and freedom for an in-depth appraisal.

Repeat reviews of a safety analysis within LLNL should be conducted by the same personnel, when possible, and some of the reviewers should have a background in safety analysis. Also, it is easier to keep track of reviews and resolutions if review forms are used. A suggested review form is shown in Fig. 3-5. Marking which comments are Significant Review Comments will help the preparation team assign pri-

REVIEW RECORD FORM

Document Title and Identifying Number _____ Revision _____ Date _____

Item No.	Reviewer's Name	Doc. Page or Sec. No.	SRC	Comment	Comment Resolution

Page No. _____ of _____

Figure 3-5. Proposed SAR review form.

orities for their resolution work.

Knowing what potential reviewers look for in a safety analysis can facilitate document preparation, review, and approval. DOE-SAN used a checklist and criteria questions to guide their review of a recent LLNL safety analysis. This checklist is given in Appendix D of this Supplement.

3.10.5 Design Criteria Considerations

Verifying compliance with safety criteria is an important part of safety analyses. The ORR recognizes SAR preparation and safety criteria compliance (e.g., DOE Order 6430.1A and 5480.5). One way to collect this information is to research any formal records of such reviews.

3.10.6 Items Requiring Further Development

Because the PSAR is done during the design stage, some information may not be complete and some safety studies may be performed during the preparation of the FSAR. Those studies or safety features for which further technical information is required to determine design adequacy or which will be used to demonstrate the margin of conservatism must be identified in the PSAR. These studies must be completed for and reported in the FSAR.

In the PSAR provide the following information:

- Identify and distinguish between those technical information development programs that will be required to determine the adequacy of a new design, and those that will be used to demonstrate the margin of conservatism of a proven design.
- Characterize the specific technical information that must be obtained to demonstrate acceptable resolution of the problems.
- Outline the program in sufficient detail to show how the information will be obtained.
- Provide a completion schedule for the program related to the projected startup date of the proposed plant.
- Discuss the design alternatives or operational restrictions available in the event that the study results do not demonstrate acceptable resolution of the problems.
- Provide reasonable assurance that the alternatives considered will be acceptable substitutes.

3.10.7 Source Term Considerations

The hazard source term is a vital part of any safety analysis. The physical system must be understood to determine how the hazard is transmitted during an event. This means determining "receptor" distances, the effect of worst-case meteorology, how much material is available for transport over certain pathways, etc. Some of this information is directly available from studies. However in most cases the available information will not apply to the specific situation being analyzed. The recommended assumptions in Ref. 3 may be used for consistency and conservatism. These assumptions should be applied carefully, since they may not apply to the specific situation, and their use may present severe economic penalties.

3.10.8 Standards and Guides

A complete list of applicable government standards and guides is given in DOE Order 5480.4. The standards, or mandatory requirements portion, can be found in *Health & Safety Manual* Supplement 1.04.

3.10.9 Future Considerations

Over the last few years, the trend has been toward more detailed safety analyses, more documentation, and more projects needing to prepare a safety analysis. Also, DOE's safety analysis process is undergoing change. One change is a modification to the independent review system to include a DOE-HQ independent oversight function at field locations. In addition, recent changes have been issued, or are being prepared, for several DOE Orders and SAN MDs that specify safety analysis standards and guidance.

One change in particular will have a significant impact on the safety analysis process. A draft DOE policy statement on safety objectives mentions, among other things:

- An intent to employ PRA as well as deterministic safety analysis.
- An intent to explore the design vulnerability of existing facilities to severe accidents beyond the original design basis.
- New philosophy for quantitative safety criteria that parallels NRC criteria.
- New quantitative safety criteria that define a term called "significant additional risk."
- New systems for controlling the documentation and review of PRAs and reliability information as well as SARs.

The draft statement is being reviewed at DOE field offices and will be released in Fall, 1988; have a two-year trial period.

This trend points out the increased attention that safety analysis is currently receiving within the DOE. The increased attention has created an unsettled atmosphere as new SARs enter the revised DOE Safety Analysis and Review System. Unfortunately, until current SARs are reviewed and approved in the new system, and the changes in DOE requirements and guidance are interpreted clearly for specific projects, this situation is likely to continue. It is clear that future safety analyses will receive more DOE and public attention.

References

1. G. E. Freeland, *Lawrence Livermore National Laboratory Earthquake Safety Program*, Lawrence Livermore National Laboratory, Livermore, CA, UCAR-10129 (1984).
2. W. J. Brynda, C. H. Scarlett, G. E. Tanguay, and P. R. Lobner, *Nonreactor Nuclear Facilities: Standards and Criteria Guide*, Rev. 1, Brookhaven National Laboratory, Associated Universities, Inc., Upton, NY, DOE/TIC-11603 (1986).
3. J. C. Elder, J. M. Graf, J. M. Dewart, T. E. Buhl, W. J. Wenzel, L. J. Walker, and A. K. Stoker, *A Guide to Radiological Accident Considerations for Siting and Design of DOE Nonreactor Nuclear Facilities*, Los Alamos National Laboratory, Los Alamos, NM, LA-10294-MS (1986).
4. G. F. Larson, *FIREONE/FIRETWO Fire Duration and Severity Calculation Software*, Westinghouse Hanford Company, Richland, WA, HEDL-7542 (1984).